Bintec
Secure IPSec Client

Version 1.0
Juli 2004

Gesamtherstellung dieses Handbuchs:
Michael Lösel
Dokumentation + Publikation
ml-service@t-online.de
Arndtstraße 5
90419 Nürnberg
0172 / 82 58 238

Wie Sie Bintec erreichen:
Bintec Access Networks GmbH
Südwestpark 94
D-90449 Nürnberg
Germany

Telephone: +49 180 300 9191 0
Fax: +49 180 300 9193 0

Haftung

Alle Programme und das Handbuch wurden mit größter Sorgfalt erstellt und nach dem Stand der Technik auf Korrektheit überprüft. Alle Haftungsansprüche infolge direkter oder indirekter Fehler, oder Zerstörungen, die im Zusammenhang mit dem Programm stehen, sind ausdrücklich ausgeschlossen. Bintec Access Networks GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslastungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie Änderungen zu diesem Produkt finden Sie unter www.bintec.de.

Inhalt

1. Produktübersicht

Dieses Handbuch beschreibt Installation, Konfiguration, Leistungsumfang und Benutzeroberfläche des Bintec Secure IPSec Client und seiner Komponenten.

Die Bintec IPSec Client Software arbeitet nach dem Prinzip einer LAN Emulation für Ethernet und unterstützt die routbaren Protokolle TCP/IP.

Weitere Informationen zur Realisierung einer sicheren VPN Kommunikation erhalten Sie auf der Bintec Website unter www.bintec.de.

1.1 Zum Umgang mit diesem Handbuch

Damit Sie sich in dieser Dokumentation schnell zurecht finden, ist im folgenden kurz ihr Aufbau dargestellt.

Das Handbuch ist in sechs größere Abschnitte untergliedert, die Step-by-Step oder dem Aufbau der grafischen Benutzeroberfläche folgend den jeweiligen Gegenstand beschreiben. Diesen Abschnitten folgen zwei Anhänge, die dem Verständnis und dem Auffinden von Fachbegriffen dienen.

Kapitel 1: Produktübersicht mit kurzer Beschreibung des Leistungsumfangs der Software
Kapitel 2: Installationsanweisungen
Kapitel 3: Beschreibung der grafischen Benutzeroberfläche, sowie der Konfigurationsmöglichkeiten
Kapitel 4: Beschreibung der in den Profil-Einstellungen aufgelisteten Parameter
Kapitel 5: Beschreibung eines Verbindungsaufbaus
Kapitel 6: Beispiele und Erklärungen, insbesondere zu IPSec
Glossar für Abkürzungen und Begriffe
Index

Querverweise sind im Text in Klammern gesetzt und geben die Verweisstelle mit dem Titel, bzw. nach einem Komma, mit dem Untertitel an.

Texte, die am Seitenrand mit einem Ausrufezeichen markiert sind, sollten besonders beachtet werden.

Weiterführende Hilfestellungen können jederzeit über die kontextsensitive Online-Hilfe abgerufen werden.

1.2 Bintec Secure IPSec Client – universelle Lösung für sichere VPN-Lösungen

Der Bintec Secure IPSec Client kann in beliebigen VPN-Umgebungen eingesetzt werden. Er kommuniziert auf der Basis des IPSec-Standards mit den Gateways verschiedenster Hersteller und ist die Alternative zu der am Markt angebotenen, einheitlichen IPSec-Client-Technologie. Die Client Software emuliert einen Ethernet LAN-Adapter. Der IPSec Client verfügt über zusätzliche Leistungsmerkmale, die dem Anwender den Einstieg in eine ganzheitliche Remote Access VPN-Lösung ermöglichen.

Der IPSec Client bietet:

☑ Unterstützung aller gängigen Betriebssysteme

☑ Einwahl über alle Übertragungsnetze

☑ Kompatibilität mit den VPN-Gateways unterschiedlichster Hersteller

☑ Integrierte Personal Firewall für mehr Sicherheit

☑ Dialer-Schutz (keine Bedrohung durch 0190er- und 0900er-Dialer)

☑ Höhere Geschwindigkeit im ISDN (Kanalbündelung)

☑ Gebührenersparnis (Kosten- und Verbindungskontrolle)

☑ Bedienungskomfort (grafische Oberfläche)

1.3 Leistungsumfang

Der IPSec Client unterstützt alle gängigen Betriebssysteme (Windows 98se, ME, NT, 2000 und Windows XP). Die Einwahl in das Firmennetz erfolgt unabhängig vom Mediatyp, d.h. neben ISDN, PSTN (analoges Fernsprechnetz), GSM, GPRS und xDSL wird auch LAN-Technik wie im WLAN (am Firmengelände und Hotspot) oder lokalen Netzwerk (z.B. Filialnetz) unterstützt. Auf diese Weise kann mit ein und demselben Endgerät von unterschiedlichen Lokationen auf das Firmennetz zugegriffen werden:

– in der Filiale über WLAN
– in der Zentrale über LAN
– unterwegs an Hotspots und beim Kunden über WLAN bzw. GPRS
– im Home Office über xDSL oder ISDN

1.3.1 Client Monitor – Grafische Benutzeroberfläche

Die grafische Oberfläche (siehe → Client Monitor) des IPSec Clients schafft Transparenz während des Einwahlvorganges und Datentransfers. Sie informiert u.a. über den aktuellen Datendurchsatz.

Der Anwender ist zu jeder Zeit darüber informiert, ob sein PC online ist und wo letztlich die Gebühren anfallen.

1.3.2 Dialer

Ein eigener Dialer ersetzt den sonst üblichen Microsoft DFÜ-Dialer. Daraus ergeben sich Vorteile gleich in mehrfacher Hinsicht:

– intelligentes Line Management (Short Hold Mode) in Wählnetzen
– Steuerung der Bandbreite (Kanalbündelung) im ISDN
– integrierte Personal Firewall-Mechanismen
– Schutz vor “automatischen Dialern”

1.3.3 Line Management

Um die Übertragungsgebühren möglichst gering zu halten, werden aktive Verbindungen automatisch unterbrochen, wenn keine Daten fließen. Liegen erneut Daten für die Übertragung vor, wird die ruhende Verbindung ohne Einwirkung des Benutzers aktiviert. Gebühren fallen immer nur dann an, wenn Daten übertragen werden. Bei der Interneteinwahl via ISDN, können beide Nutzkanäle gebündelt werden (dynamische Linkzuschaltung), falls für den Transfer größerer Datenmengen eine hohe Übertragsrate benötigt wird.

Ein weiteres Instrument zur Kostenkontrolle ist die intelligente Verbindungssteuerung. Hier werden Online-Sessions nach Zeit, nach Anzahl der Verbindungsaufbauten oder Gebühreneinheiten angezeigt und bei Bedarf überwacht.

1.3.4 Personal Firewall

Der IPSec Client verfügt über alle erforderlichen Personal Firewall Funktionalitäten um den PC-Arbeitsplatz umfassend gegenüber Angriffen aus dem Internet und anderer LAN-Teilnehmer (WLAN oder LAN) zu schützen. Weiter besteht keine Möglichkeit, dass der Dialer von automatischen 0190er- und 0900er-Dialern für ungewollte Verbindungen missbraucht wird. Die wesentlichen Security-Mechanismen sind IP-NAT und Protokollfilter. NAT (Network Address Translation) ist ein Security-Standard zum Verbergen der individuellen IP-Adressen gegenüber dem Internet. NAT bewirkt eine Übersetzung der von außen sichtbaren Adresse in entsprechende Client-Adressen und umgekehrt. Ankommende Datenpakete werden auf der Basis eines ausgeklügelten Filterings nach genau definierten Eigenschaften überprüft und bei Nichtübereinstimmung abgewiesen. Das heißt: Der Internet-Port des jeweiligen Rechners wird vollständig getarnt und der Aufbau von unerwünschten Verbindungen unmöglich.

1.3.5 PKI-Unterstützung

Die Zugangssicherheit zum PC und damit dem Firmennetz kann durch den Einsatz elektonischer Zertifikate in Form von Software (PKCS#12) oder Smart Cards (PKCS#11, CT-API, PC/SC) erhöht werden. Der IPSec Client unterstützt hierfür die Einbindung in eine PKI (Public Key Infrastruktur).

Public Key Infrastruktur

Public-Key-Infrastrukturen (PKI) beschreiben ein weltweit genutztes Verfahren, um zwischen beliebigen Kommunikationspartnern auf elektronischem Wege Schlüssel sicher auszutauschen. Die PKI bedient sich dabei sogenannter Schlüsselpärchen aus jeweils einem öffentlichen und einem privaten Schlüssel. In der Welt des elektronischen, globalen Informationsaustausches wird so eine Vertrauensbasis aufgebaut, wie wir sie in der traditionellen Geschäftswelt auf Papierbasis kennen. Die digitale Signatur in Verbindung mit Datenverschlüsselung ist das elektronische Äquivalent zur händisch geleisteten Unterschrift und belegt Ursprung sowie die Authentizität von Daten und Teilnehmer.

Eine PKI basiert auf digitalen Zertifikaten, die - von einer öffentlichen Zertifizierungsstelle (Trust Center) ausgestellt - als persönliche “elektronische Ausweise” fungieren und idealerweise auf einer Smart Card abgespeichert sind. Sicherheitsexperten und der IETF (Internet Engineering Task Force) sind sich darüber einig, dass ein nachhaltiger Schutz vor Man-In-The-Middle-Attacken nur durch den Einsatz von Smart Cards mit Zertifikaten erreicht werden kann.

Smart Card

Smart Cards sind die ideale Ergänzung für hochsichere Remote Access-Lösungen. Sie bieten doppelte Sicherheit beim Login-Vorgang, nämlich Wissen über PIN (Persönliche Identifikations Nummer) und Besitz der Smart Card. Der Anwender identifiziert sich mit der Eingabe der PIN eindeutig als rechtmäßiger Besitzer (Strong Authentication). Die PIN ersetzt das Passwort und die Eingabe der User-ID (Basistechnologie für Single Sign On). Der Anwender weist sich nur noch gegenüber der Smart Card aus. Der Check gegenüber dem Netz erfolgt zwischen Smart Card und Security-System. Alle sicherheitsrelevanten Operationen laufen vollständig im Inneren der Karte - also außerhalb des PCs - ab. Das System ist neben individuellen Anpassungen an Schutzmechanismen offen für multifunktionalen Einsatz (z. B. als Company Card). Auch biometrische Verfahren lassen sich integrieren.

2. Installation

Die Installation der Secure Software für Windows-Systeme erfolgt komfortabel über Setup. Der Installationsablauf ist für alle Versionen des Secure Clients identisch. Im folgenden ist die Installation für Windows 98/ME und Windows NT/2000/XP beschrieben.

Bevor Sie die Software installieren, müssen, zur vollen Funktionsfähigkeit die Installationsvoraussetzungen, wie im folgenden Kapitel beschrieben, erfüllt sein.

2.1 Installationsvoraussetzungen

Betriebssystem

Die Software kann auf Computern (min. 32 MB RAM) mit den Betriebssystemen Microsoft Windows 98se / Millenium, Windows NT (3.5 oder höher) ab Service Pack 4 (oder höher) oder Windows 2000 oder Windows XP installiert werden.

Halten Sie für die Dauer der Installation unbedingt die Datenträger (CD oder Disketten) für das jeweils im Einsatz befindliche Betriebssystem bereit, um Daten für die Treiberdatenbank des Betriebssystems nachladen zu können!

Zielsystem

Die Parameter für das Zielsystem werden über die Profil-Einstellungen eingegeben. Entsprechend der möglichen Verbindungsarten des Clients muss das Zielsystem eine der folgenden Verbindungsarten unterstützen: ISDN, PSTN (analoges Modem), LAN over IP oder PPP over Ethernet.

Lokales System

Eines der folgenden Kommunikationsgeräte und der entsprechende Treiber muss auf dem Client-PC installiert sein.

- **ISDN-Adapter (ISDN)**

  Der ISDN-Adapter muss die ISDN CAPI 2.0 unterstützen. Wenn Sie PPP Multilink nutzen, kann die Software bis zu 8 ISDN B-Kanäle (je nach Kanalanzahl des Adapters) bündeln. Prinzipiell kann jeder ISDN-Adapter, der die ISDN-Schnittstelle CAPI 2.0 unterstützt, eingesetzt werden. (Für gewöhnlich wird die CAPI bei der Installation eines ISDN-Adapters automatisch eingerichtet.)

- **Analoges Modem (Modem)**

  Für die Kommunikation über Modem (PSTN) muss das Modem korrekt installiert sein, sowie Modem Init. String und COM-Port Definition zugewiesen sein. Das Modem muss den Hayes-Befehlssatz unterstützen.

  Ebenso können Mobiltelefone für die Datenkommunikation genutzt werden, nachdem die zugehörige Software installiert wurde, die sich für den Client genauso darstellt wie ein analoges Modem. Als Schnittstelle zwischen Handy und PC kann die serielle Schnittstelle, die IR-Schnittstelle (Infrarot) oder Bluetooth genutzt werden. Je nach Übertragungsart (GSM, V.110, GPRS, UMTS oder HSCSD) muss die Gegenstelle über

die entsprechende Einwahlplattform verfügen. Der in die Modemkonfiguration des Secure Clients einzutragende Initialisierungs-String ist vom ISP oder dem Hersteller des Mobiltelefons zu beziehen.

- **LAN-Adapter (LAN over IP)**

  Um die Client-Software mit der Verbindungsart “LAN (over IP)” in einem Local Area Network betreiben zu können, muss zusätzlich zum bereits installierten LAN-Adapter (Ethernet oder Token Ring) kein weiterer Adapter installiert werden. Die Verbindung der LAN-Clients ins WAN stellt ein beliebiger Access Router her. Einzige Voraussetzung: IP-Verbindung zum Zielsystem muss möglich sein. Die VPN-Funktionalität liefert die Client Software.
  Adapter für ein wireless LAN (WLAN-Adapter) werden genauso behandelt wie normale LAN-Adapter. Auch für WLAN muss als Verbindungsart “LAN (over IP)” gewählt werden.

- **xDSL-Modem (xDSL (PPPoE))**

  Die Verbindungsart “xDSL (PPPoE)” setzt voraus, dass eine Ethernet-Karte installiert und darüber ein xDSL-Modem mit Splitter korrekt angeschlossen ist.

- **xDSL (AVM - PPP over CAPI)**

  Die Verbindungsart “AVM – PPP over CAPI” kann gewählt werden, wenn eine AVM Fritz! DSL-Karte eingesetzt wird. Im Feld “Rufnummer (Ziel)” in der Gruppe “Netzeinwahl” können für die Verbindung über CAPI noch AVM-spezifische Intitialisierungskommandos eingetragen werden.
  Unter Windows Betriebssystemen wird jedoch empfohlen den Standard “xDSL (PPPoE)” zu verwenden, da damit direkt über die Netzwerkschnittstelle mit der Karte kommuniziert wird.
  Bei Verwendung der AVM Fritz! DSL-Karte wird keine separate zusätzliche Netzwerkkarte benötigt.

Voraussetzungen für den Einsatz von Zertifikaten

Wenn Sie die Software mit Zertifizierung (X.509) nutzen, so müssen folgende Voraussetzungen erfüllt sein:

- **TCP/IP**

  Das Netzwerk-Protokoll TCP/IP muss auf dem Rechner installiert sein.

- **Chipkartenleser**

  Wenn Sie die “Erweiterte Authentisierung” (Strong Authentication) mit Smart Cards nutzen wollen, muss ein Chipkartenleser an Ihr System angeschlossen sein. Die Client Software unterstützt automatisch alle Chipkartenleser, die PC/SC-konform sind. Diese Chipkartenleser werden nur in der Liste der Chipkartenleser aufgenommen, nachdem

der Leser angeschlossen und die zugehörige Treiber-Software installiert wurde. Die Client Software erkennt dann den Chipkartenleser nach einem Boot-Vorgang automatisch. Erst dann kann der installierte Leser ausgewählt und genutzt werden.

Dazu stellen Sie nach dem ersten Start des Monitors den Chipkartenleser ein unter “Konfiguration → Zertifikate”. Nachdem Sie die Smart Card in den Chipkartenleser gesteckt haben, können Sie Ihre PIN eingeben..

■ Chipkartenleser (CT-API-konform)

Wenn Sie einen CT-API-konformen Chipkartenleser nutzen, beachten Sie bitte folgendes:

☑ Mit der aktuellen Software werden Treiber für die Modelle Kobil B0/B1, Kobil KAAN, SCM Swapsmart und SCM 1x0 (PIN Pad Reader) mitgeliefert. Diese Chipkartenleser können im Monitor unter “Konfiguration → Zertifikate” eingestellt werden. Sollte der Chipkartenleser mit den mitgelieferten Treibern nicht funktionieren oder ein anderer Chipkartenleser installiert sein, wenden Sie sich unbedingt an den Hersteller des Chipkartenlesers, bzw. konsultieren Sie die entsprechende Website bezüglich aktueller Hardware-Treiber, um den aktuellsten CT-API-Treiber zu erhalten und zu installieren. Nehmen Sie außerdem folgende Einstellung in der Client Software vor:

☑ Editieren Sie die Datei NCPPKI.CONF, befindlich im Windows\System-Verzeichnis (unter Windows 95/98) oder System32-Verzeichnis (unter Windows NT/2000) mit einem ASCII-Editor, indem Sie als “Modulname” den Namen des angeschlossenen Chipkartenlesers (xyz) eintragen und als DLLWIN95 bzw. DLLWINNT den Namen des installierten Treibers eintragen. (Der Standardname für CT-API-konforme Treiber ist CT32.DLL).

Wichtig: Nur die Treiber sind in der Liste sichtbar, die mit “visible = 1” auf sichtbar gesetzt wurden!

Modulname	= SCM Swapsmart (CT-API)	→ xyz
DLLWIN95	= scm20098.dll	→ ct32.dll
DLLWINNT	= scm200nt.dll	→ ct32.dll

☑ Nach einem Boot-Vorgang erscheint der von Ihnen eingetragene “Modulname” im Monitor-Menü unter “Konfiguration → Zertifikate → Chipkartenleser”. Selektieren Sie nun diesen Chipkartenleser.

■ Chipkarten

Folgende Chipkarten werden unterstützt:

☐ Signtrust

☐ NetKey 2000

☐ TC Trust (CardOS M4)

Soft-Zertifikate (PKCS#12)

Statt einer Smart Card können auch Soft-Zertifikate genutzt werden.

Chipkarten oder Token (PKCS#11)

Mit der Software für die Smart Card oder den Token werden Treiber in Form einer PKCS#11-Bibliothek (DLL) mitgeliefert. Diese Treiber-Software muss zunächst installiert werden. Anschließend muss die Datei NCPPKI.CONF editiert werden.

☑ Editieren Sie die Datei NCPPKI.CONF, befindlich im Windows\System-Verzeichnis (unter Windows 95/98) oder System32-Verzeichnis (unter Windows NT/2000) mit einem ASCII-Editor, indem Sie als “Modulname” den Namen des angeschlossenen Lesers oder Tokens (xyz) eintragen. Als PKCS#11-DLL muss der Name der DLL eingegeben werden. Der zugehörige “Slotindex” ist herstellerabhängig (Standard = 0).

Wichtig: Nur die Treiber sind in der Liste sichtbar, die mit “visible = 1” auf sichtbar gesetzt wurden!

Modulname = xyz
PKCS#11-DLL = Name der DLL
Slotindex =

☑ Nach einem Boot-Vorgang erscheint der von Ihnen eingetragene “Modulname” im Monitor-Menü unter “Konfiguration → Zertifikate → Chipkartenleser”. Selektieren Sie nun diesen Chipkartenleser oder Token.

2.2 Installation der Client Software

Die Software wird unter den Betriebssystemen Windows 98/ME und Windows NT/2000/XP mit geringfügigen Unterschieden auf ähnliche Weise installiert.

Sie können die Software in Form einer ZIP-Datei als Download von den Bintec Internetseiten unter www.bintec.de beziehen.

Bitte beachten Sie bei der Installation des IPSec Clients unter Windows XP:

Die Systemeigenschaften des Betriebssystems Windows XP sind bei Neueinrichtung restriktiv beschaffen. Sie sind standardmäßig so eingestellt, dass bei der Installation von Treiber-Software, die nicht von Microsoft lizenziert wurde, ein MS-spezifischer sogenannter “Windows-Logo-Test” durchgeführt wird, in dessen Folge das Betriebssystem davor warnt, die Treiber-Software zu installieren. Dem kann auf zwei Arten begegnet werden:

☑ Ändern Sie die restriktive Standardeinstellung des Systems. Unter “System – Systemeigenschaften – Hardware – Gerätemanager – Treibersignaturoptionen” ändern Sie das Vorgehen von Windows auf “Ignorieren - Software unabhängig von Zulassung installieren”!

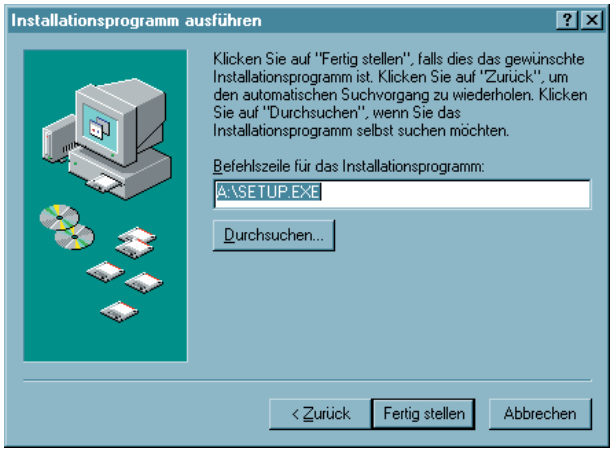
☑ Nehmen Sie die obige Einstellungsänderung nicht vor, erscheint während des Setups nach dem Kopieren der Dateien eine Meldung, die vor der Installation des Client Adapters warnt – ignorieren Sie diese Meldung und klicken Sie auf “Installation fortsetzen”!

2.2.1 Standard-Installation

Die ZIP-Datei, die Sie mit einem Download oder mit der CD erhalten haben, kopieren Sie auf die Festplatte des PCs und entpacken sie in einem Verzeichnis Ihrer Wahl. Beim Entpacken werden automatisch die Verzeichnisse “DISK1”, ”DISK2”, “DISK3” etc. angelegt. Wählen Sie im Windows-Hauptmenü ”Start → Einstellungen → Systemsteuerung.”

In der Windows-Systemsteuerung wählen Sie “Software” oder “Neue Programme hinzufügen”. Klicken Sie anschließend auf den Button zum Installieren von “CD oder Diskette”.

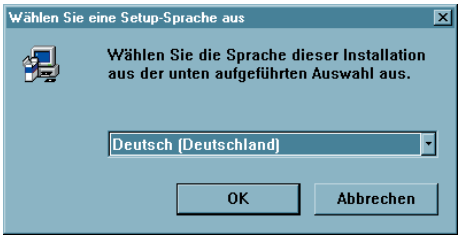
Wenn nebenstehendes Fenster erscheint klicken Sie auf “Weiter”.



Im daraufhin erscheinenden Fenster klicken Sie auf “Durchsuchen”, um im Verzeichnis mit der ZIP-Datei das Unterverzeichnis Disk1 und dort das Programm SETUP.EXE zu suchen.

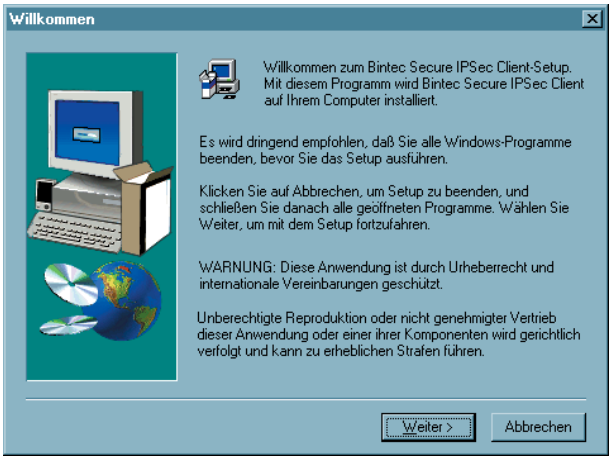
Wenn “SETUP.EXE” angezeigt wird, klicken Sie auf ”Fertigstellen”.

→ *weiter nächste Seite*

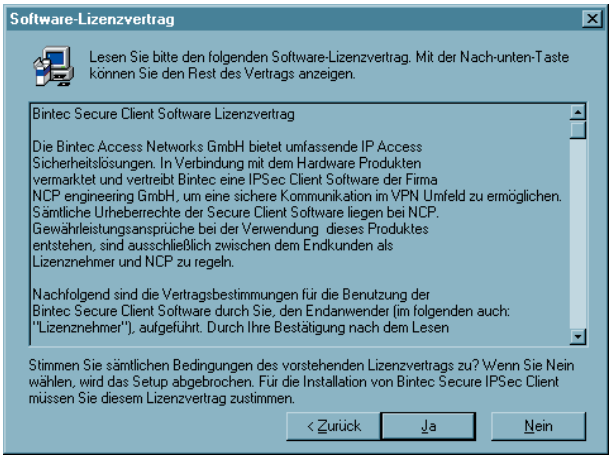


Im folgenden Fenster können Sie die Setup-Sprache auswählen. Klicken Sie danach auf “OK”.

Anschließend bereitet das Setup-Programm den Install-Shield Assistenten vor, mit dessen Hilfe die Installation fortgesetzt wird.



Lesen Sie bitte die Hinweise im Willkommen-Fenster des Setup-Programms bevor Sie auf “Weiter” klicken.



Anschließend werden die Lizenzbedingungen gezeigt. Stimmen Sie dem Vertag mit “Ja” zu, sonst wird die Installation abgebrochen.

→ *weiter nächste Seite*

Haben Sie noch keine Lizenz erworben, so wählen Sie in diesem Fenster die Installation einer Testversion.

Sollten Sie eine Testversion installieren, so ist diese vom Zeitpunkt der Installation für 30 Tage gültig und kann danach nicht mehr gestartet werden.

→ *weiter nächste Seite*

Haben Sie eine Lizenz für die Software erworben, so wählen Sie “Installation als Vollversion” und klicken ”Weiter”.

Die Vollversion der Software wird aktiviert, indem Sie anschließend Aktivierungsschlüssel und Seriennummer Ihrer Software-Lizenz in die dafür vorgesehenen Felder eintragen. (Aktivierungsschlüssel und Seriennummer befinden sich auf dem Beipackzettel zur CD-Verpackung!)

Sind diese Codes korrekt eingetragen, wird der “Weiter”-Button in diesem Fenster (links) aktiviert. Mit ”Weiter” schalten Sie die Software für den uneingeschränkten Funktionsumfang frei. Ihre Software ist damit voll einsatzfähig.

→ *weiter nächste Seite*

Wenn Sie eine “Normale Installation” vornehmen, ist das Setup mit diesem Fenster (links) abgeschlossen.

Nehmen Sie eine “Benutzerdefinierte Installation” vor, so können Sie weitere Einstellungen vornehmen

Im folgenden Fenster der “Benutzerdefinierten Installation” bestimmen Sie den Programmordner für die Client Software.
(Standard ist “Bintec Secure IPSec Client”).

Außerdem kann das Icon auf dem Desktop angezeigt werden.

Zu den weiteren Einstellungen bezüglich Ihres Gateways sind nähere Informationen von Ihrem Administrator oder Internet Service Provider nötig.

→ *für Windows 98/ME weiter unter 2.2.4*

→ *für Windows NT/2000/XP weiter unter 2.2.5*

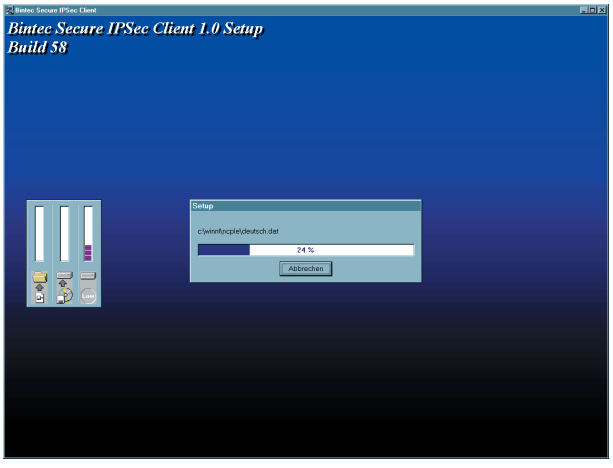
Im folgenden unterscheiden sich die Installationsschritte unter Windows 98/ME und Windows NT/2000/XP geringfügig.

2.2.2 Benutzerdefinierte Installation und Abschluss unter Windows 98/ME

Mit DHCP (Dynamic Host Control Protocol) zu kommunizieren, bedeutet, dass Sie für jede Session automatisch eine IP-Adresse zugewiesen bekommen. In diesem Fall klicken Sie auf “IP-Adresse wird von Server vergeben”.

Wenn Sie die “IP-Adresse selbst festlegen”, geben Sie in diesem Fenster die IP-Adressen ein. Bitte beachten Sie: Ist bereits eine Netzwerkkarte mit Default Gateway installiert, so muss der Eintrag “Default Gateway” hier gelöscht werden. Es darf nur eine Netzwerkkarte mit Default Gateway installiert sein. Die DNS-Adresse bitte nur eintragen, wenn Sie sie von Ihrem Provider oder Systemadministrator zur Verfügung gestellt bekommen haben.

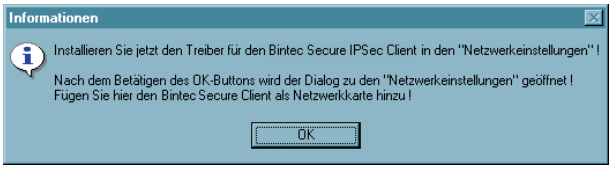
Ende der benutzerdefinierten Installation!
→ zum Abschluss weiter auf der nächsten Seite



[Ist auf Ihrem Rechner bereits eine Client Software installiert, müssen sie sich nun entscheiden, ob Sie die Software deinstallieren oder updaten möchten (siehe → Update und Deinstallation).]

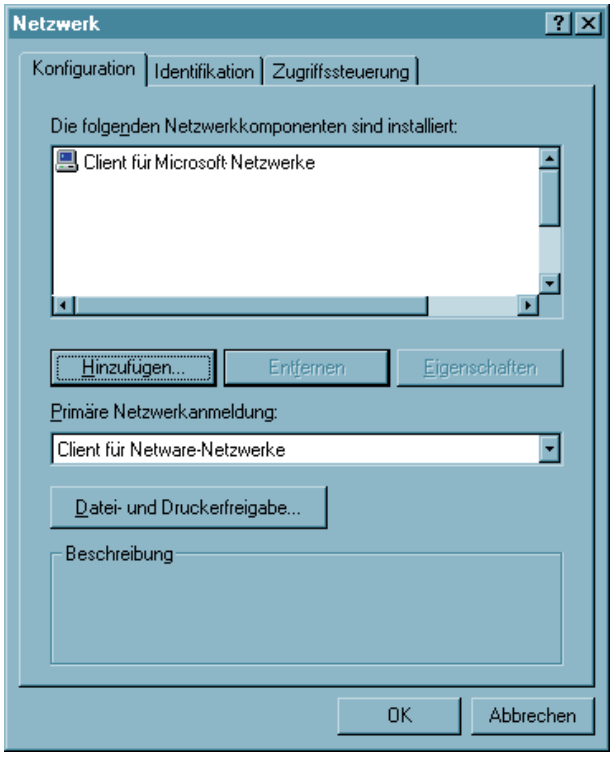
Anschließend werden die Dateien geladen und eingespielt.

Nachdem alle benötigten Dateien von den Installationsdisketten eingespielt wurden und die Programmgruppe angelegt wurde, klicken Sie auf “Beenden”, um das Setup abzuschließen.



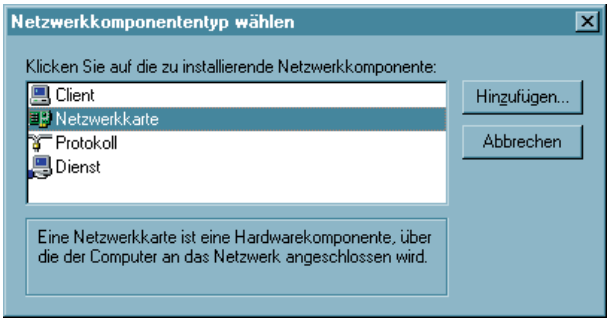
Jetzt muss nur noch der Treiber (Bintec Secure Client) als Adapter installiert werden. Fahren Sie fort indem Sie auf “OK” klicken.

→ *weiter nächste Seite*

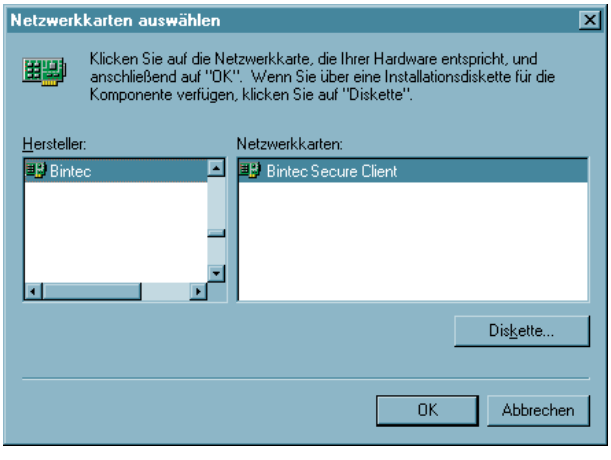


Nach dem Betätigen des OK-Buttons wird der Dialog “Netzwerk” geöffnet (siehe links). Klicken Sie ”Hinzufügen” ...

(Bei Windows ME wird ein entsprechender, gesonderter Dialog zu “Hardware hinzufügen” eingeblendet.)

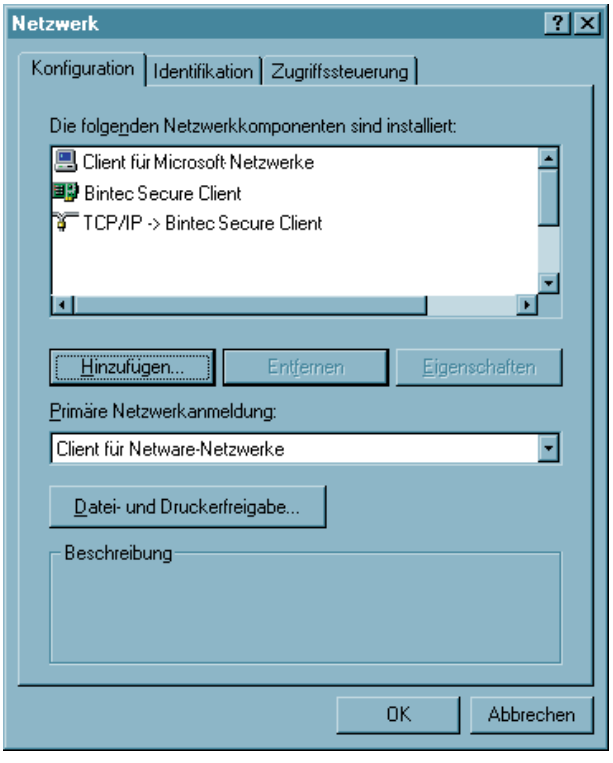


... wählen Sie “Netzwerkkarte” und betätigen Sie nochmals ”Hinzufügen”.



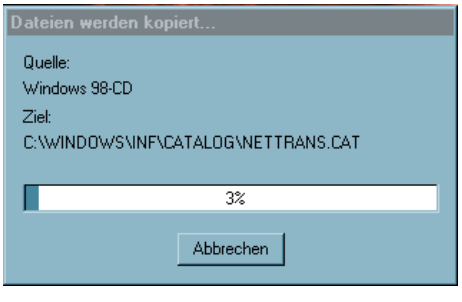
Unter der Rubrik “Hersteller” wählen Sie ”Bintec” aus und wählen dazu den Treiber auf der rechten Seite. Nach dem Betätigen des OK-Buttons wird der Treiber installiert. Damit ist die Installation der Client Software mit Setup unter Windows 98/ME abgeschlossen.

→ *weiter nächste Seite*

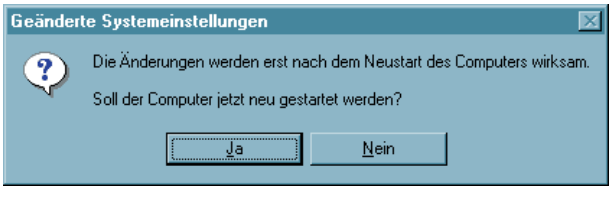


Anschließend ist die gewählte Netzwerkkarte mit dem TCP/IP-Protokoll im Netzwerk verfügbar (siehe links).

Unter Umständen müssen nun noch Dateien vom Windows-Datenträger kopiert werden...



Legen Sie dazu die CD ein oder geben Sie den Pfad an.



Anschließend betätigen Sie den Ja-Button und booten Sie damit das System!

2.2.3 Benutzerdefinierte Installation und Abschluss unter Windows NT/2000/XP

Mit DHCP (Dynamic Host Control Protocol) zu kommunizieren, bedeutet, dass Sie für jede Session automatisch eine IP-Adresse zugewiesen bekommen. In diesem Fall klicken Sie auf “IP-Adresse wird von Server vergeben”.

Wenn Sie die “IP-Adresse selbst festlegen”, geben Sie in diesem Fenster die IP-Adressen ein. Bitte beachten Sie: Ist bereits eine Netzwerkkarte mit Default Gateway installiert, so muss der Eintrag “Default Gateway” hier gelöscht werden. Es darf nur eine Netzwerkkarte mit Default Gateway installiert sein. Die DNS-Adresse bitte nur eintragen, wenn Sie sie von Ihrem Provider oder Systemadministrator zur Verfügung gestellt bekommen haben.

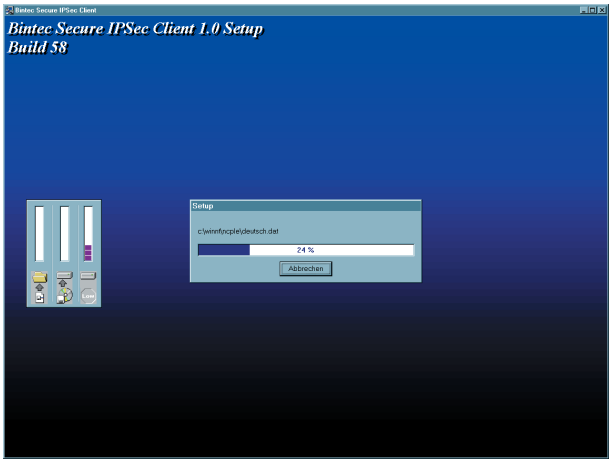
→ *weiter nächste Seite*

Schließlich können Sie angeben, welche weiteren Protokolle und Dienste Sie installieren wollen. Halten Sie dafür den Datenträger zu Ihrem Betriebssystem bereit, da eventuell Treiber von diesem Datenträger benötigt werden. Mit “Weiter” schließen Sie die Benutzerdefinitionen ab.

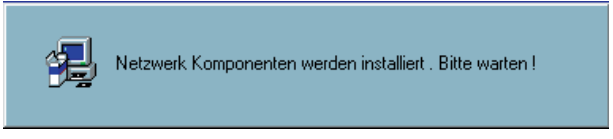
Ende der benutzerdefinierten Installation!

Sie können anschließend entscheiden, ob vor dem Windows-Logon an einer remote Domain die Verbindung zum Network Access Server aufgebaut werden soll. Für diesen Verbindungsaufbau müssen Sie gegebenenfalls die PIN für ihr Zertifikat und das (nicht gespeicherte) Passwort für die Client Software eingeben. Nachdem die Verbindung zum NAS hergestellt wurde, können Sie sich an die remote Domain anmelden. Diese Anmeldung erfolgt dann bereits verschlüsselt.

→ *weiter nächste Seite*



Danach werden die Dateien der Client Software eingespielt.



Anschließend werden die Netzwerkkomponenten installiert.

Damit ist die Installation der Client Software unter Windows NT/2000/XP abgeschlossen. Die neuen Einstellungen werden erst wirksam, wenn Sie den Computer neu starten. Klicken Sie “Ja, Computer jetzt neu starten” und betätigen Sie den Beenden-Button, um Ihr System zu booten.

Entfernen Sie die Datenträger aus den Laufwerken!

Hinweise für Benutzerberechtigungen finden Sie in der Datei SECCLIENT_NTD.TXT (siehe auch “Zum Betrieb des Secure Clients unter Windows NT/2000/XP”)

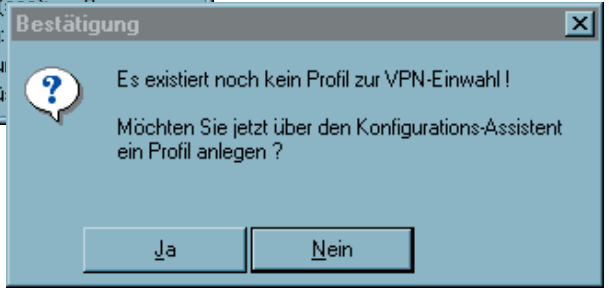
2.2.4 Zum Betrieb des IPSec Clients unter Windows NT/2000/XP

Um mit der Client Software arbeiten zu können, ohne Administratorrechte zu besitzen, müssen Schreib- und Leserechte für folgende Dateien eingerichtet sein:

- ☑ Alle Dateien im Unterverzeichnis NCPLE des Betriebssystems Windows NT müssen Leserechte besitzen, die Datei NCPPHONE.CFG benötigt zusätzlich Schreibrechte. Zudem müssen in diesem Verzeichnis Dateien erzeugt werden können.
- ☑ Die Datei NCPBM.DAT benötigt Lese- und Schreibrechte (Statistik, Budgetmanager).
- ☑ Die Datei NCP.DB im Verzeichnis WINDOWS\SYSTEM32\DRIVERS benötigt ebenfalls Schreib- und Leserechte.

2.3 Vor der Inbetriebnahme

Nach der Installation zeigt sich der Client Monitor auf dem Bildschirm. Um den Client nutzen zu können, muss zunächst unter den Profil-Einstellungen ein Eintrag erzeugt werden, d.h. das Profil zu einem Zielsystem definiert werden, zu dem eine IPSec-Verbindung hergestellt werden kann.



Sie können dazu den angebotenen Assistenten benutzen, wenn Sie im Bestätigungsfenster auf “Ja” klicken (siehe Bild rechts).

Der Assistent kann auch zu einem späteren Zeitpunkt gestartet werden. Dazu wird der Menüpunkt “Profil-Einstellungen” im Hauptmenü des Monitors unter “Konfiguration” aktiviert. (Siehe dazu → 3. Client Monitor, Konfiguration, Profil-Einstellungen.)

Für die weitergehende Konfiguration eines Profils beachten Sie bitte die Beschreibungen unter “3. Client Monitor, Profil-Einstellungen” und “4. Konfigurationsparameter, IPSec-Einstellungen”.

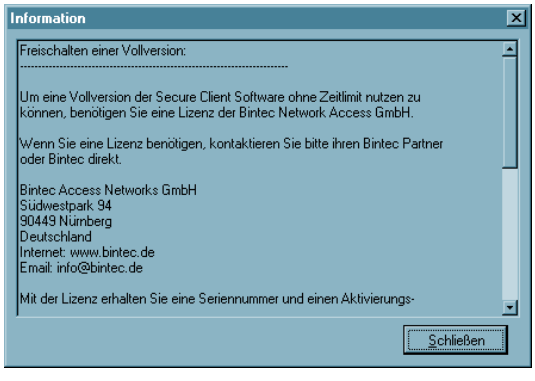
Erst nach der Einrichtung eines Profils kann eine Verbindung zum eingestellten Zielsystem hergestellt werden. Siehe dazu “5. Eine Verbindung herstellen”.

Um die Einstellungen Ihres IPSec Clients auf Funktionstüchtigkeit hin zu überprüfen, bietet Bintec einen entsprechenden öffentlichen Testzugang. Eine detaillierte Konfigurationsanleitung zur Nutzung dieses VPN-Testzugangs in Verbindung mit dem Bintec Secure IPSec Client finden Sie unter www.bintec.de.

2.4 Freischalten einer Vollversion

Wenn Sie bisher eine Testversion der Client Software benutzt haben und nun eine Vollversion nachinstallieren möchten, gehen Sie bitte wie folgt vor:

1. Aktivieren Sie in der Windows-Programmgruppe “Bintec Secure IPSec Client” das Programm ”Secure Client Popup”. Damit erscheint nebenstehendes Fenster.



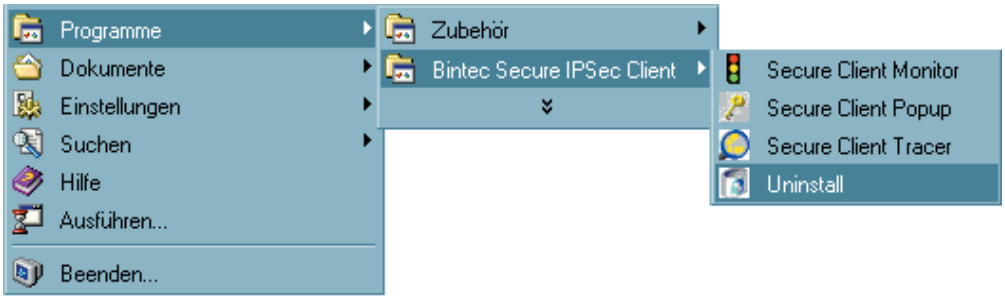
2. Unter dem Menüpunkt “Info” finden Sie die nötigen Angaben, um eine Lizenz erwerben zu können.

3. Unter dem Menüpunkt “Aktivierungsschlüssel” können Sie die Testversion freischalten. Vor dem Bild des Popup-Menüs erscheint ein Fenster, worin Sie Aktivierungsschlüssel und Seriennummer Ihrer Vollversion eintragen können. Tragen Sie nun Aktivierungsschlüssel und Seriennummer ein. Wenn Sie korrekt eingetragen sind, können Sie den OK-Button bedienen. Damit ist eine Vollversion freigeschaltet.

2.5 Deinstallation

Zum Entfernen der Client Software kann zwischen zwei Optionen gewählt werden:

1. Sie wählen im Windows-Startmenü aus der Programmgruppe "Bintec Secure IPSec Client" das Programm "Uninstall" (siehe Bild unten).



Wenn Sie die Sicherheitsabfrage "Bintec Secure IPSec Client deinstallieren" mit "Ja" beantworten, entfernt das Uninstall Shield Programm die Client Software von Ihrem PC.

2. Sie wählen im Windows-Startmenü nach den "Einstellungen" die Gruppe “Systemsteuerung”. Klicken Sie nun auf “Software” und wählen Sie den Client aus der Liste. Klicken Sie dann auf den Button mit “Hinzufügen/Entfernen”. Das Uninstall Shield Programm löscht nun die Client Software von Ihrem PC.

Wichtig: Nachdem die Komponenten entfernt wurden, sind die Profil-Einstellungen des Clients erhalten geblieben, so dass sie für neuere Versionen des Clients genutzt werden können. Um die Dateien vollständig vom PC zu löschen, müssen Sie sie per Hand gelöscht werden, je nach Windows-Betriebssystem aus einem der beiden Verzeichnisse:
`C:\Windows\ncple`
oder
`C:\WINNT\ncple`

3. Client Monitor

Wenn die Software installiert wurde, kann der Monitor über das Start-Menü → Programme → Bintec Secure IPSec Client → Secure Client Monitor aktiviert werden. Damit öffnet sich das Fenster des Monitors auf dem Bildschirm.

Hinweis: Wenn der Monitor geladen wurde, erscheint er entweder auf dem Bildschirm oder, wenn er dort nicht dargestellt wird, in der Taskleiste.

Der Monitor hat 4 wichtige Funktionen:

☑ den aktuellen Status der Kommunikation wiederzugeben

☑ den Verbindungsmodus einzustellen

☑ die Limits der Verbindungssteuerung bestimmen

☑ die Definition und Konfiguration der Profile zur Anwahl an ein Zielsystem

3.1 Die Benutzung der Monitors

Anwahl über das Profil an das Zielsystem

Sobald die Software installiert mit einem Profil korrekt konfiguriert wurde (siehe unten 3.2.3 Konfiguration), kann die Anwahl an dieses Zielsystem stattfinden.

Das gewunschte Profil wird über die Auswahl-Box unter dem Hauptmenü oder nach Klick auf die rechte Maustaste aus einer Liste gewählt (siehe nebenstehendes Bild).

Um eine Verbindung über das selektierte Profil herzustellen, ist es nicht nötig, den Client Monitor eigens zu starten oder die Anwahl manuell durchzufuhren.

Lediglich die gewünschte Applikations-Software muss gestartet werden.

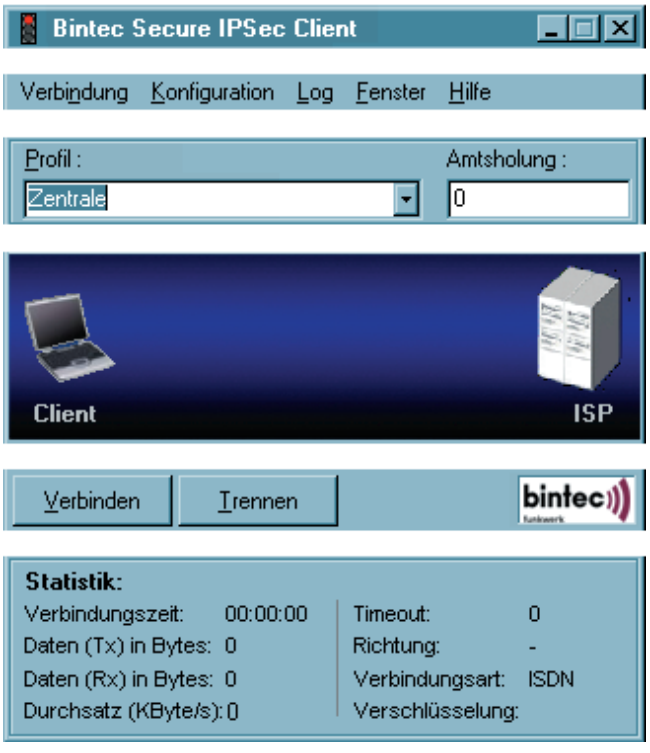
Die Verbindung wird dann, entsprechend den Parametern des Profils, automatisch aufgebaut (siehe → Verbindungssteuerung, Verbindungsaufbau, automatisch). Daneben ist es auch moglich, manuell die Verbindung herzustellen, indem Sie im Monitor den Hauptmenüpunkt “Verbindung” anklicken und “Verbinden” wählen. Alternativ kann auch der Button “Verbinden” angeklickt werden (siehe → Verbindungsaufbau).

Eine bestehende Verbindung (siehe → Bild oben) wird mit einem dicken grünen, durchgehenden Balken zwischen Client und Server dargestellt, unter dem der Text “Verbindung ist hergestellt” eingeblendet wird. Gleichzeitig wird die (Icon-)Ampel grün. Damit werden Sie darauf aufmerksam gemacht, dass fur eine Remote-Verbindung Gebühren anfallen.

3.1.1 Die Oberfläche des Client Monitors

Der Client Monitor besteht aus:

- einer Titelzeile mit Ampelanzeige,
- der Hauptmenüleiste,
- der Profilauswahl mit einem Feld für die Amtsholung,
- dem grafischen Statusfeld zur Anzeige des Verbindungsstatus,
- der Buttonleiste mit “Verbinden” und “Trennen”
- und einem Statistikfeld



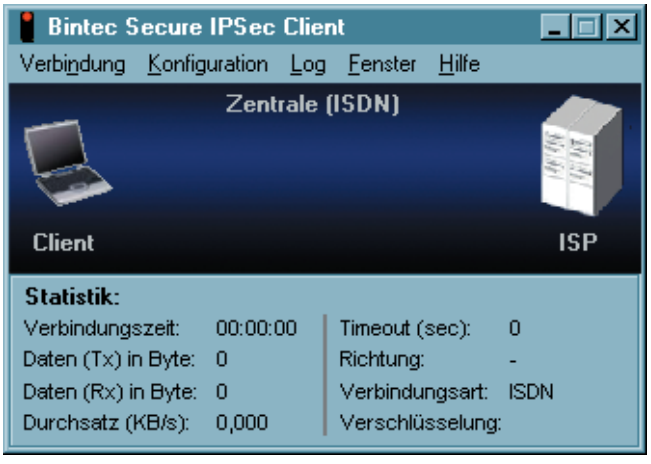
Die Benutzeroberfäche ist Windows-konform gestaltet und der Bedienung anderer Windows-Anwendungen angepasst.

Der Monitor kann bedient werden über die Pulldown-Menüs der Menüleiste, über die Buttons der Buttonleiste oder über das Kontextmenü (rechte Maustaste).

3.1.2 Das Erscheinungsbild des Monitors

Je nach gewählter Einstellung im Monitor-Menu “Fenster” erscheint der Monitor nach Ausblenden seiner Bestandteile (siehe → 3.2.5 Fenster) in verschiedenen Größen.

Das Verbindungsmedium lässt sich im Statistikfeld ablesen oder kann bei der Namensvergabe an das Profil mit eingegeben werden, sodass sie auch im grafischen Statusfeld erscheint.



Modifikationen der Oberfläche

Bitte beachten Sie, dass das Erscheinungsbild des Client Monitors vom Administrator verändert werden kann. Dies betrifft insbesondere die Menüpunkte “Verbindungs-Informationen”, “Zertifikate”, “Verbindungssteuerung” und “Logon Optionen”. Auch Parameterfelder des Telefonbuchs und einzelne Parameter können vom Administrator ausgeblendet bzw. auf “nicht konfigurierbar” gesetzt werden. Die ausgeblendeten und deaktivierten Features und Parameter erleichtern Ihnen den Umgang mit der Software und haben weder Einfluss auf die Leistungsfähigkeit der Software noch auf Ihre Arbeit. Beachten Sie dazu den Abschnitt 3.3 Konfiguration, 3.3.8 Konfigurations-Sperren.

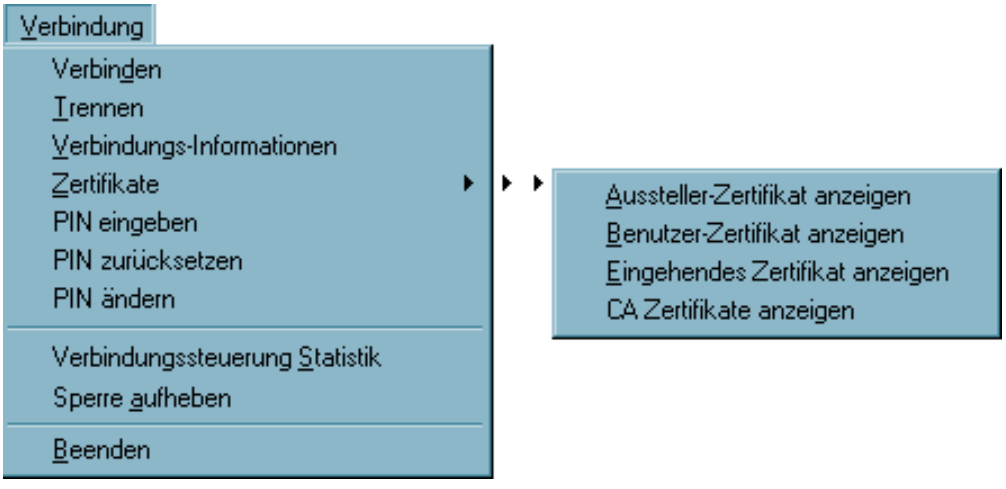
3.2 Monitor-Bedienung

Diese Beschreibung folgt den Menüpunkten in der Menüleiste.

Die Hauptmenüpunkte in der Menüleiste von links nach rechts sind:

- ☐ Verbindung
- ☐ Konfiguration
- ☐ Log
- ☐ Fenster
- ☐ Hilfe

3.2.1 Verbindung



Unter diesem Menüpunkt befinden sich die Kommandos zum Aufbau und Trennen einer Verbindung, Informationsfenster zum aktuellen Verbindungsaufbau sowie zur Darstellung der eingesetzten Zertifikate. Die PIN für das Zertifikat kann hier eingegeben und ggf. geändert werden. Außerdem kann hier die Statistik der Verbindungsteuerung abgelesen werden und gegebenenfalls die Sperre der Verbindungssteuerung gelöst werden, wenn ein von Ihnen gesetztes Limit überschritten wurde.

Verbinden

Eine Verbindung wird aufgebaut. Eine Verbindung kann nur aufgebaut werden, wenn ein “Profil” aus der Liste der “Profil-Einstellungen” selektiert ist. Das selektierte “Profil” wird in der Monitoroberfläche unter der Menüleiste angezeigt.

Wenn Sie die Funktion “Verbinden” wählen, wird die Anwahl an das Ziel über das ausgewählte Profil manuell durchgeführt.

Wenn Sie, je nach Profil, die Verbindung manuell oder automatisch herstellen wollen, so können Sie dies in den Profil-Einstellungen mit dem Parameter “Verbindungsaufbau” im Feld “Verbindungsdauer” definieren (siehe → Profil-Einstellungen, Line Management, Verbindungsaufbau).

Trennen

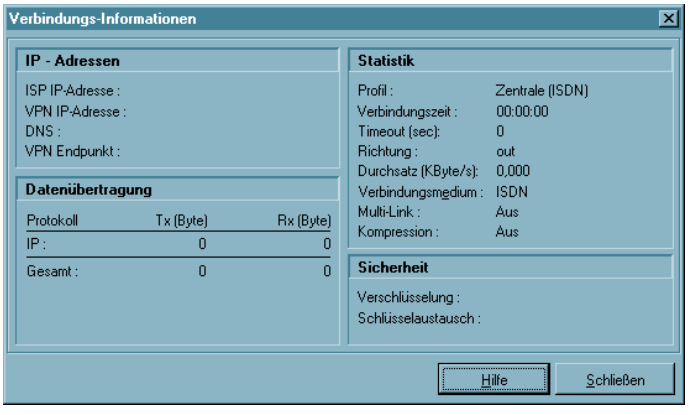
Eine Verbindung kann manuell abgebaut werden mit der Funktion “Trennen” im Pulldown-Menü oder nach Klick auf die rechte Maustaste.

Wenn die Verbindung abgebaut wurde, wechseln die Signallampen des Monitors für die gesamte Offline-Dauer von grün zu rot.

Verbindungs-Informationen

Wenn Sie den Menüpunkt “Verbindungs-Informationen” anklicken, werden statistische Werte gezeigt. Darüber hinaus aber auch welche Security-Schlüssel (SSL mit Zertifikat, Blowfish ...) verwendet werden und welche IP-Adressen über PPP-Verhandlung zwischen Client und Server ausgetauscht werden. Der Monitor mit den Verbindungs-Informationen hat keinerlei Einfluss auf die Funktionen der Client-Software.

Die Verbindungs-Informationen können vom Administrator ausgeblendet werden, sodass der Menüpunkt nicht aktiviert werden kann.



Sind die Verbindungs-Informationen ausgeblendet, so können die wichtigsten Daten aus den Feldern der Datenübertragung, derStatistik und der Sicherheit auch aus dem Statistik-Fenster des Clients abgelesen werden (siehe → 3.2.5 Fenster, Statistik anzeigen).

Verbindungszeit

Als Verbindungszeit wird die gesamte Zeit angezeigt, während der Sie an ein bestimmtes Gateway angewählt sind, unabhangig von irgendwelchen Timeouts. Der Wert für die Verbindungszeit wird nur dann auf null (0) gesetzt, wenn Sie eine Verbindung zu einem anderen Gateway herstellen oder den PC erneut booten.

Timeout

Der Monitor zeigt die Zeit an, die bis zum nächsten Timeout noch verbleibt. Unmittelbar nachdem der letzte Datenaustausch erfolgt ist (einschließlich Handshake) beginnt die Uhr fur den Timeout zu laufen. Der Timeout-Wert kann im Telefonbuch unter Line Managment eingestellt werden.

Richtung

Unter dieser Rubrik wird die Richtung der Kommunikation wie folgt angezeigt:
Out = ein ausgehender Ruf wird auf diesem Kanal registriert
In = ein ankommender Ruf wird auf diesem Kanal registriert.

Durchsatz

Die angezeigte Zahl schwankt entsprechend dem aktuellen Datendurchsatz.

Verbindungsmedium

Folgende Verbindungsmedium werden unterstützt: ISDN-, Modem, LAN over IP, xDSL (PPPoE), xDSL (AVM - PPP over CAPI), GPRS und PPTP.

Multilink

Besteht die Verbindung über mehrere ISDN-B-Kanale, so wird hier “on” angezeigt.

Kompression

Kompression wird immer vom Gateway definiert. IPSec-Kompression wird mit “IPSec Compression (LZS)” angezeigt.

Verschlüsselung

Der verwendete Verschlüsselungsalgorithmus wird angezeigt. Folgende Typen werden unterstützt: AES, Blowfish, 3DES. Die Verschlüsselungsart wird vom Zentralsystem vorgegeben.

Schlüsselaustausch

Hier wird angezeigt, auf welche Art der Austausch des Session Keys erfolgt:

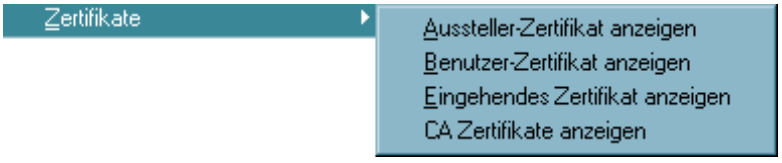
Static Key — Der Schlüssel muss am Client und am Zentralsystem ubereinstimmen. Er wird in der Profil-Einstellung unter “Identität” eingetragen

IKE (IPSec) — Zur Übertragung des Session Keys wird der verschlüsselte Kontrollkanal der Phase-1-Verhandlung verwendet.

Rx und Tx Bytes

Rx und Tx Bytes zeigt die Datenmenge an, die gesendet (out) und empfangen (in) wird. Die Gesamtmenge (Total) und die nach Protokoll unterschiedenen Datenmnegen werden in Bytes angezeigt (1 Byte = 1 Zeichen).

Zertifikate



Im Pulldown-Menü “Verbindung” finden Sie den Menüpunkt “Zertifikate” mit den Menüabzweigungen “Konfiguration”, “Aussteller-Zertifikat anzeigen”, “Eingehendes Zertifikat anzeigen” und “CA-Zertifikate anzeigen”.

Zertificate (Certificates) werden von einer CA (Certification Authority) mittels PKI-Manager (Software) ausgestellt und auf eine Smart Card (Chipkarte) gebrannt. Diese Smart Card enthält u.a. mit den Zertifikaten digitale Signaturen, die ihr den Status eines digitalen Personalausweises verleihen.

Aussteller-Zertifikat anzeigen

Wenn Sie sich das Aussteller-Zertifikat anzeigen lassen, können Sie sehen welche Merkmale zur Erstellung des Zertifikats genutzt wurden, z.B. die eindeutige E-Mail-Adresse.

Aussteller (CA)	=	Benutzer und Aussteller eines Aussteller-Zertifikates sind für gewöhnlich identisch (selfsigned certificate). Der Aussteller des Aussteller-Zertifikats muss mit dem Aussteller des Benutzer-Zertifikats identisch sein (siehe → Benutzer-Zertifikat anzeigen).
Seriennummer	=	Nach der Seriennummer werden die Zertifikate mit den in der Revocation List der Certification Authority gehaltenen verglichen.
Gültigkeitsdauer	=	Die Gültigkeitsdauer der Zertifikate ist beschränkt. Die Gültigkeitsdauer eines Aussteller(Root)-Zertifikats ist in aller Regel länger als die eines Benutzer-Zertifikats. Mit dem Erlöschen der Gültigkeit des Aussteller-Zertifikats erlischt automatisch die Gültigkeit eines vom gleichen Aussteller ausgestellten Benutzer-Zertifikates.
Fingerprint	=	Hash-Wert. Der mit dem Private Key der CA verschlüsselte Hash-Wert ist die Signatur des Zertifikats.

Benutzer-Zertifikat anzeigen

Wenn Sie sich Ihr Benutzer-Zertifikat anzeigen lassen, können Sie sehen welche Merkmale zur Erstellung des Zertifikats genutzt wurden, z.B. die eindeutige E-Mail-Adresse.

Austeller (CA)	=	Der Aussteller Ihres Benutzer-Zertifikates muss mit dem Aussteller des Aussteller-Zertifikates identisch sein. (siehe → Aussteller-Zertifikat anzeigen).
Seriennummer	=	Nach der Seriennummer werden die Zertifikate mit den in der Revokation List der Certification Authority gehaltenen verglichen.
Gültigkeitsdauer	=	Die Gültigkeitsdauer der Zertifikate ist beschränkt. Die Gültigkeitsdauer eines Aussteller(Root)-Zertifikats ist in aller Regel länger als die eines Benutzer-Zertifikats. Mit Erlöschen der Gültigkeit geht auch die Funktion des Zertifikats verloren.
Fingerprint	=	Hash-Wert. Der mit dem Private Key der CA verschlüsselte Hash-Wert ist die Signatur des Zertifikats.

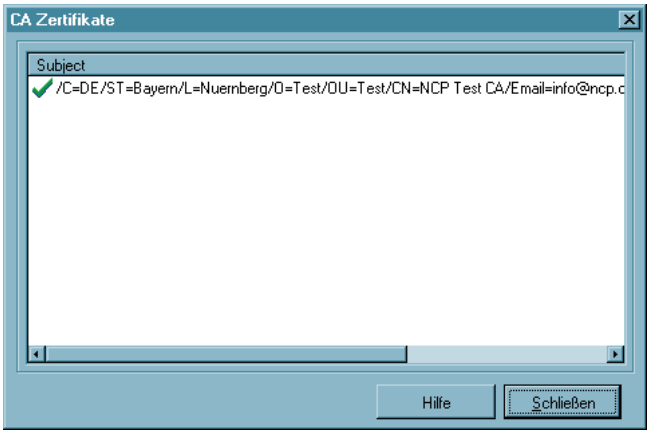
Eingehendes Zertifikat anzeigen

Anzeige des Zertifikats, das bei der SSL-Verhandlung von der Gegenstelle (VPN Gateway) übermittelt wird. Sie können z.B. sehen, ob Sie den hier gezeigten Aussteller in der Liste Ihrer CA-Zertifikate (siehe unten) aufgenommen haben.

Ist das eingehende Benutzer-Zertifikat einer der CAs aus der Liste “CA-Zertifikate anzeigen” nicht bekannt, kommt die Verbindung nicht zustande.

Sind keine CA-Zertifikate im Windows-Verzeichnis NCPLE\CACERTS\ gespeichert, so findet keine Überprüfung statt.

CA-Zertifikate anzeigen



Mit der Client Software werden mehrere Aussteller-Zertifikate unterstützt (Multi CA-Unterstützung). Dazu müssen die Aussteller-Zertifikate im Windows-Verzeichnis NCPLE\CACERTS\ gesammelt werden. Im Monitor des Clients wird die Liste der eingespielten CA-Zertifikate angezeigt unter dem Menüpukt "Verbindung → Zertifikate → CA-Zertifikate".

Wird das Aussteller-Zertifikat einer Gegenstelle empfangen, so ermittelt der Client den Aussteller und sucht anschließend das Aussteller-Zertifikat, zunächst auf Smart Card oder PKCS#12-Datei, anschließend im Verzeichnis NCPLE\CACERTS\.

Ist das Aussteller-Zertifikat nicht bekannt, kommt die Verbindung nicht zustande (No Root Certificate found). Sind keine CA-Zertifikate im Windows-Verzeichnis NCPLE\CACERTS\ vorhanden, so wird keine Verbindung unter Einsatz von Zertifikaten zugelassen.

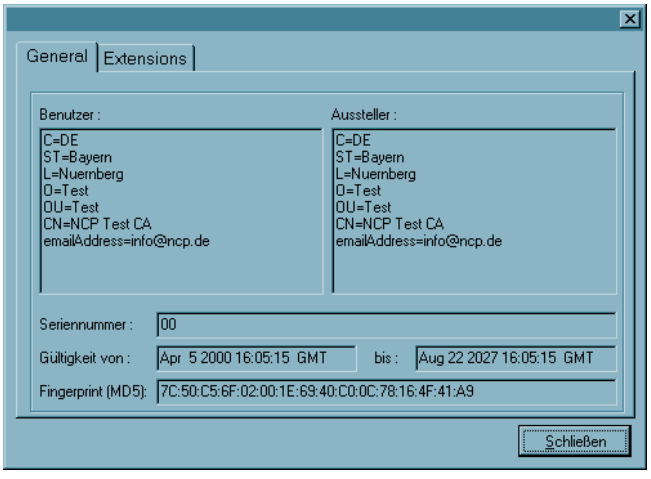
Anzeige und Auswertung von Erweiterungen bei eingehenden Zertifikaten und CA-Zertifikaten

Zertifikate können Erweiterungen (Extensions) erfahren. Diese dienen zur Verknüpfung von zusätzlichen Attributen mit Benutzern oder öffentlichen Schlüsseln, die für die Verwaltung und den Betrieb der Zerifizierungshierarchie und der Sperrlisten (Revocation Lists) benötigt werden. Prinzipiell können Zertifikate eine beliebige Anzahl von Erweiterungen inklusive privat definierter beinhalten. Die Zertifikats-Erweiterungen (Extensions) werden von der ausstellenden Certification Authority in das Zertifikat geschrieben.

Für den IPSec Client und das Gateway sind drei Erweiterungen von Bedeutung:

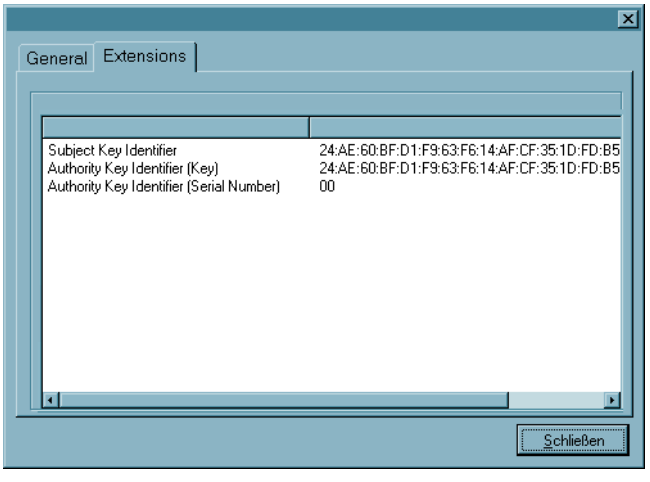
- ☐ extendedKeyUsage
- ☐ subjectKeyIdentifier
- ☐ authorityKeyIdentifier

Anzeige der Erweiterungen (Extensions)



Um sich die Erweiterungen eines eingehenden oder CA-Zertifikats anzeigen zu lassen, kann wie folgt vorgegangen werden:

Das CA-Zertifikat, dessen Erweiterungen angezeigt werden sollen, muss mit einem Doppelklick im Fenster für CA-Zertifikate (siehe oben) geöffnet werden. Damit wird nebenstehendes Anzeigefeld mit den allgemeinen Daten (General) geöffnet.



Für das jeweils eingehende Zertifikat wird dieses Feld bereits geöffnet, nachdem “Eingehendes Zertifikat anzeigen” im Zertifikats-Menü gewählt wurde.

Das Ansichtsfeld “General” zeigt die allgemeinen Zertifikatsdaten (siehe Bild oben).

Das Ansichtsfeld “Extensions” zeigt die Zertifikatserweiterungen, sofern sie vorhanden sind (siehe Bild links).

Auswertung der Erweiterungen (Extensions)

extendedKeyUsage

Befindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung extendedKeyUsage so prüft der IPSec Client, ob der definierte erweiterte Verwendungszweck die “SSL-Server-Authentisierung” ist. Ist das eingehende Zertifikat nicht zur Server-Authentisierung vorgesehen, so wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

Bitte beachten Sie, dass die SSL-Server-Authentisierung richtungsabhängig ist. D.h. der Initiator des Tunnelaufbaus prüft das eingehende Zertifikat der Gegenstelle, das, sofern die Erweiterung extendedKeyUsage vorhanden ist, den Verwendungszweck “SSL-Server-Authentisierung” beinhalten muss

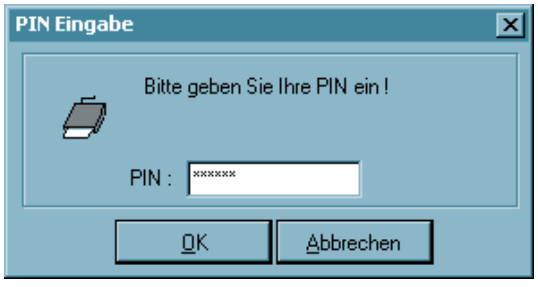
subjectKeyIdentifier / authorityKeyIdentifier

Ein keyIdentifier ist eine zusätzliche ID (Hashwert) zum CA-Namen auf einem Zertifikat. Der authorityKeyIdentifier (SHA1-Hash über den public Key des Ausstellers) am eingehenden Zertifikat muss mit dem subjectKeyIdentifier (SHA1-Hash über den public Key des Inhabers) am entsprechenden CA-Zertifikat übereinstimmen. Kann kein CA-Zertifikat gefunden werden, wird die Verbindung abgelehnt.

Der keyIdentifier kennzeichnet den öffentlichen Schlüssel der Zertifizierungsstelle und somit nicht nur eine, sondern gegebenenfalls eine Reihe von Zertifikaten. Damit erlaubt die Verwendung des keyIdentifiers eine größere Flexibilität zum Auffinden eines Zertifizierungspfades. Außerdem müssen die Zertifikate, die den keyIdentifier in der authorityKeyIdentifier-Erweiterung besitzen, nicht zurückgezogen werden, wenn die CA sich bei gleichbleibendem Schlüssel ein neues Zertifikat ausstellen lässt.

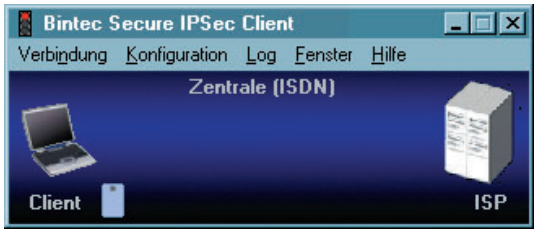
PIN eingeben

Die PIN-Eingabe kann bereits vor einem Verbindungsaufbau erfolgen, nachdem der Monitor gestartet wurde. Wird zu einem späteren Zeitpunkt eine Verbindung aufgebaut, die ein Zertifikat erfordert, so kann dann die PIN-Eingabe unterbleiben – es sei denn, die Konfiguration zum Zertifikat verlangt dies (siehe → Konfiguration, Zertifikate).



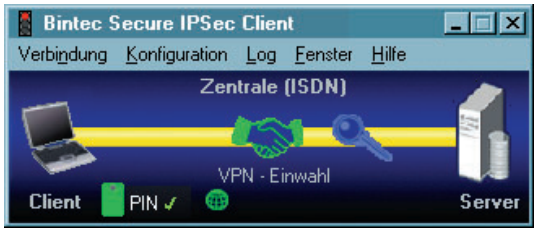
Haben Sie den Menüpunkt “Verbindung – PIN eingeben” gewählt, kann in das geöffnete Eingabefeld die PIN (mindestens 6-stellig) eingegeben werden und mit “OK” bestätigt werden. Die Ziffern der PIN werden als Sterne “*” am Bildschirm dargestellt.

Sofern die PIN noch nicht vor einem Verbindungsaufbau eingegeben wurde, erscheint der Dialog zur PIN-Eingabe spätestens wenn die erste Verbindung zu einem Ziel hergestellt werden soll, das die Verwendung eines Zertifikats erfordert. Nachfolgend kann bei einem wiederholten manuellen Verbindungsaufbau die PIN-Eingabe unterbleiben, wenn dies so konfiguriert wurde (siehe → Konfiguration, Zertifikate).



Wenn Sie den IPSec Client zur Verwendung einer Smart Card oder eines PKCS#11-Moduls konfiguriert haben (siehe → Konfiguration, Zertifikate), erscheint im Statusfeld ein hellblaues Symbol für die Smart Card (Bild links). Wenn Sie Ihre Smart Card in das Lesegerät gesteckt haben, ändert sich die Farbe des Symbols von hellblau zu grün.

Wurde der IPSec Client zur Verwendung eines Soft-Zertifikats konfiguriert (siehe → Konfiguration, Zertifikate), erscheint im Statusfeld kein eigenes Symbol.



Wurde die PIN korrekt eingegeben, so wird dies in der Monitoroberfläche mit einem grünen Haken hinter “PIN” dargestellt (Bild links).

Fehlerhafte Eingaben und falsche PINs werden nach ca. 3 Sekunden mit einer Fehlermeldung “Falsche PIN!” quittiert. Ein Verbindungsaufbau ist dann nicht möglich.

Bitte beachten Sie, dass bei mehrmaliger falscher PIN-Eingabe eine Smart Card oder ein Token gesperrt werden kann. Wenden Sie sich in diesem Fall an Ihren Administrator.

Erst nach korrekter PIN-Eingabe kann der Verbindungsaufbau erfolgen.

Wird eine Smart Card oder ein Token während des laufenden Betriebs entfernt, findet standardmäßig ein Verbindungsabbau statt.

Der Verbindungsabbau muss jedoch nicht bei gezogener Chipkarte erfolgen! Ob “Kein Verbindungsabbau bei gezogener Chipkarte” erfolgt, wird über das Hauptmenü des Monitors unter dem Menüpunkt “Konfiguration – Zertifikate” eingestellt.

Die Richtlinien zur PIN-Eingabe können im Hauptmenü unter “Konfiguration → Zertifikate” festgelegt werden (siehe → Konfiguration, Zertifikate, PIN-Richtlinie). Diese Richtlinien müssen auch befolgt werden, wenn die PIN geändert wird (siehe → Verbindung, PIN ändern).

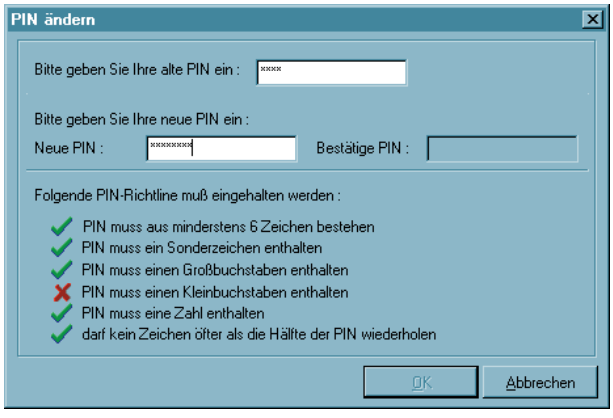
Bitte beachten Sie: Unter dem Menüpunkt “PIN ändern” kann die PIN für eine Smart Card oder ein Soft-Zertifikat geändert werden, wenn vorher die richtige PIN eingegeben wurde. Ohne die vorherige Eingabe einer gültigen PIN wird dieser Menüpunkt nicht aktiviert.

■ PIN zurücksetzen

Dieser Menüpunkt ist nur aktiv, wenn die PIN bereits richtig eingegeben wurde, d. h. das Zertifikat für die aufzubauende Verbindung genutzt werden soll.

Wird die PIN zurückgesetzt, kann dieses Zertifikat für einen Verbindungsaufbau nicht mehr genutzt werden, bis die dazugehörige PIN wieder richtig eingegeben wurde.

PIN ändern



Unter diesem Menüpunkt kann die PIN für eine Smart Card oder ein Soft-Zertifikat geändert werden, wenn vorher die richtige PIN eingegeben wurde (siehe → PIN eingeben). Ohne die vorherige Eingabe einer gültigen PIN wird dieser Menüpunkt nicht aktiviert.

Aus Sicherheitsgründen – um die PIN-Änderung nur für den authorisierten Benutzer zuzulassen –, muss nach Öffnen dieses Dialogs die noch gültige PIN ein zweites Mal eingegeben werden. Die Ziffern der PIN werden in diesem und den nächsten Eingabefeldern als Sterne "*" dargestellt.

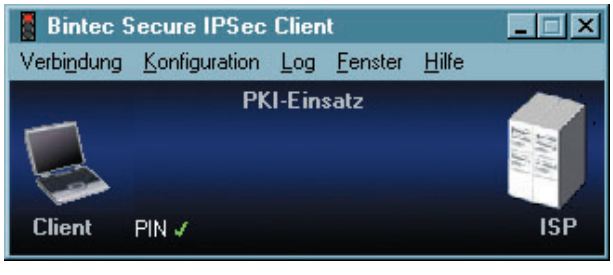
Anschließend geben Sie Ihre neue PIN ein und bestätigen diese durch Wiederholung im letzten Eingabefeld. Mit Klick auf "OK" haben Sie Ihre PIN geändert.

Die einzuhaltenden PIN-Richtlinien werden unter den Eingabefeldern eingeblendet. Sie können im Hauptmenü unter "Zertifikate → PIN-Richtlinien" eingestellt werden (Bild oben).

PIN-Eingabezwang nach Abmeldung oder Sleep-Mode

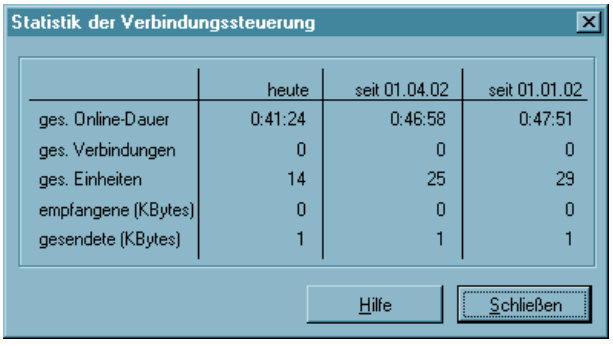
Wird unter den Betriebssystemen Windows NT/2000/XP der Benutzer gewechselt, wird der PIN-Status zurückgesetzt und die PIN muss erneut eingegeben werden. Wechselt der Computer in den Sleep-Modus, wird ebenfalls der PIN-Status zurückgesetzt.

PIN-Status im Client Monitor



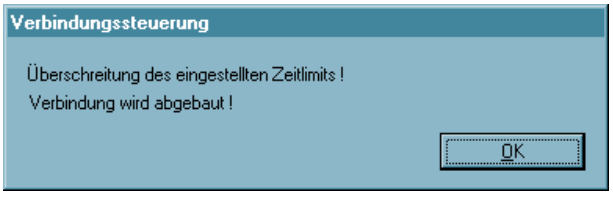
Wurde die PIN bereits eingegeben, erscheint im Monitor die Einblendung "PIN" mit einem grünen Haken. Wurde die PIN noch nicht korrekt eingegeben, fehlt der kleine grüne Haken.

Verbindungssteuerung Statistik



Die Statistik gibt Ihnen Auskunft über Ihre Datenkommunikation. In ihr werden sowohl gesondert als auch aufaddiert die gesamten Online-Zeiten, die gesamte Anzahl der Verbindungen und die gesamten Einheiten, sowie empfangene und gesendete Kbytes für den aktuellen Tag, den laufenden Monat und das laufende Jahr angezeigt.

Sperre aufheben



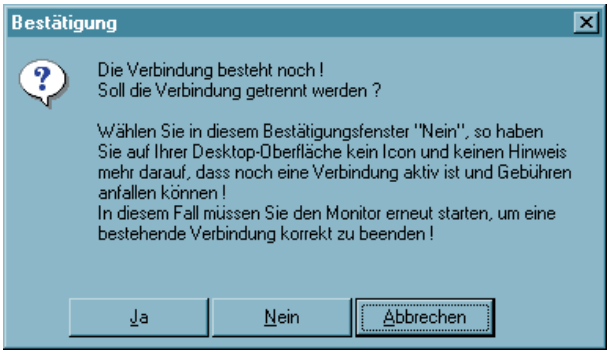
Je nachdem, wie die Verbindungssteuerung eingestellt ist, erhalten Sie bei Überschreiten eines Limits Meldungen auf dem Bildschirm. Wird ein Limit überschritten und die Verbindung automatisch abgebaut, wird eine Sperre aktiv, die jeden weiteren Verbindungsaufbau unterbindet (siehe → “Verbindung”-Menü im Monitor).

Eine Verbindung kann erst dann wieder neu aufgebaut werden, wenn Sie die “Sperre aufheben”.

■ Beenden (des Monitors)

Wurde die Verbindung bereits getrennt, beendet ein Klick auf diesen Menüpunkt oder der Schließen-Button den Monitor. Besteht noch eine Verbindung, kann nach Klick auf diesen Menüpunkt oder den Schließen-Button der Monitor ebenfalls beendet werden. Beachten Sie jedoch unbedingt, dass die Verbindung dabei nicht automatisch getrennt wird. Soll die möglicherweise kostenpflichtige Verbindung bestehen bleiben, obwohl der Monitor beendet wird, so wird dazu ausdrücklich eine Bestätigung von der Software verlangt.

Klicken Sie in diesem Bestätigungsfenster auf “Nein”, so haben Sie auf Ihrer Desktop-Oberfläche kein Icon und keinen Hinweis mehr darauf, dass noch eine Verbindung aktiv ist und Gebühren anfallen können! In diesem Fall müssen Sie den Monitor erneut starten, um eine bestehende Verbindung korrekt zu beenden!



3.2.2 Konfiguration

Unter diesem Menüpunkt können sämtliche Einstellungen für die Arbeit mit dem IPSec Client vorgenommen werden, die länger als eine Session bestehen sollen. Dies betrifft das Anlegen der Profile, die Konfiguration der IPSec-Verbindungen, die Wahl der Verbindungsart, sowie die Eingabe einer Amtsholung für Anschlüsse an Telekommunikationsanlagen.

Darüber hinaus kann eigens konfiguriert werden, wie Zertifikate genutzt werden sollen, wie die Verbindungssteuerung arbeiten soll und welche Konfigurations-Rechte der Benutzer erhält.

Um die Einstellungen Ihres IPSec Clients auf Funktionstüchtigkeit hin zu überprüfen, bietet Bintec einen entsprechenden öffentlichen Testzugang. Eine detaillierte Konfigurationsanleitung zur Nutzung dieses VPN-Testzugangs in Verbindung mit dem Bintec Secure IPSec Client finden Sie unter www.bintec.de.

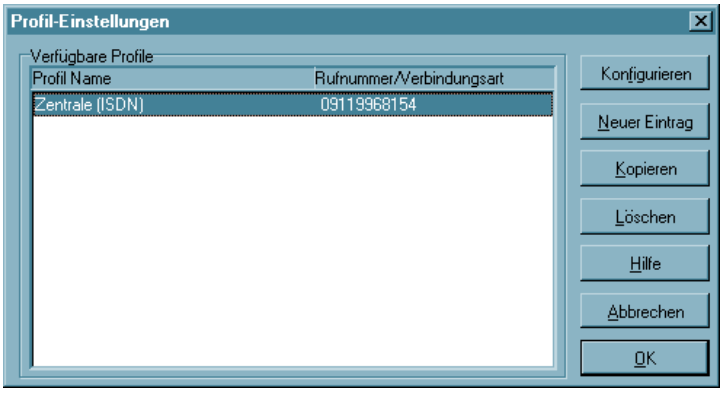
Profil-Einstellungen

Die Einträge der Profil-Einstellungen

Bei einer Erstinstallation der IPSec Client Software ist noch kein Profil vorhanden. In diesem Fall wird automatisch ein Konfiguartions-Assistent eingeblendet, der Ihnen hilft, eine Konfiguration anzulegen. Damit wird zugleich das erste Profil der IPSec Client Software angelegt. Dieser Assistent wird auch gestartet bei Klick auf “Neuer Eintrag” (siehe unten, “Neuer Eintrag – Profil”).

Mit den Profil-Einstellungen kann die Parametrisierung für die Zielsysteme (Profil) durchgeführt und die Übertragungsart, den Benutzeranforderungen entsprechend, bis ins Detail konfiguriert werden.

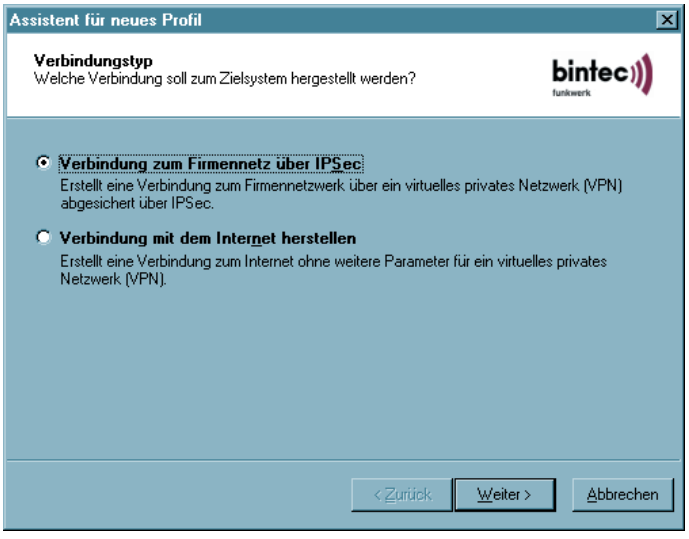
Nachdem Sie auf “Profil-Einstellungen” im Monitor-Menü “Konfiguration” geklickt haben, öffnet sich das Menü und zeigt in einer Liste der bereits verfügbaren Profile deren Namen und die Rufnummern der zugehörigen Zielsysteme.



Auf der rechten Seite der Profil-Einstellungen sind Buttons angebracht zu folgenden Funktionen: Konfigurieren, Neuer Eintrag, Kopieren, Löschen, OK, Hilfe und Abbrechen.

Neuer Eintrag – Profil

Um ein neues Profil zu definieren, klicken Sie auf “Profil-Einstellungen”. Wenn sich das Fenster des Menüs öffnet klicken Sie auf “Neuer Eintrag”. Jetzt legt der “Assistent für ein neues Profil” mit Ihrer Hilfe ein neues Profil an. Dazu blendet er die unbedingt notwendigen Parameter auf. Wenn Sie die Einträge in diesen Feldern vorgenommen haben, ist ein neues Profil angelegt. Für alle weiteren Parameterfelder des Profils werden Standardwerte eingetragen.



Mit dem Konfigurations-Assistenten können Verbindungen mit dem Internet oder zum Firmennetz rasch hergestellt werden. Je nach Auswahl des gewünschten Verbindungstyps wird das Profil nach wenigen Konfigurationsabfragen angelegt.

Im folgenden die jeweils notigen Daten zur Konfiguration:

Verbindung zum Firmennetz über IPSec:

→ Profil-Name
→ Verbindungsmedium
→ Zugangsdaten fur Internet-Dienstanbeiter (Benutzername, Passwort, Rufnummer)
→ VPN-Gateway-Parameter (Tunnelendpunkt IP-Adresse)
→ Zugangsdaten fur VPN-Gateway (XAUTH, Benutzername, Passwort)
→ IPSec-Konfiguration (Exch. Mode, PFS-Gruppe, Kompression)
→ Statischer Schlüssel (Preshared Key), ohne Zertifikat (IKE ID-Typ, IKE ID)
→ IP-Adressen-Konfiguration (IP-Adresse des Clients, DNS/WINS-Server)
→ Firewall-Einstellungen

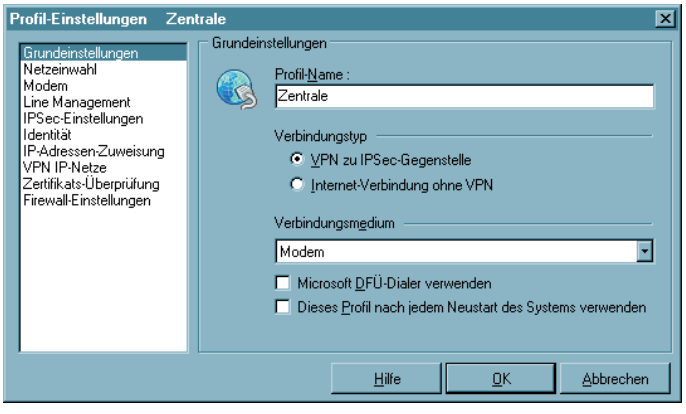
Verbindung mit dem Internet herstellen:

→ Profil-Name
→ Verbindungsmedium
→ Zugangsdaten fur Internet-Dienstanbeiter (Benutzer, Passwort, Rufnummer)

Das neue Profil erscheint nun in der Liste der Profile mit dem von Ihnen vergebenen Namen. Wenn keine weiteren Parameter-Einstellungen nötig sind, können Sie die Liste mit Ok schließen. Das neue Profil ist im Monitor sofort verfügbar. Es kann im Monitor ausgewählt werden und über das Menü “Verbindung → Verbinden” kann das zugehörige Ziel sofort angewählt werden.

Konfigurieren – Profil

Um die (Standard-)Werte eines Profils zu editieren, wählen Sie mit der Maus das Profil, dessen Werte Sie ändern möchten, und klicken anschließend auf “Konfigurieren”. Die Profil-Einstellungen zeigen nun in ihrem linken Fenster eine Liste von Begriffen, denen jeweils ein Parameterfeld zugeordnet ist:



Grundeinstellungen
Netzeinwahl
Modem
Line Management
IPSec-Einstellungen
Identität
IP-Adressen-Zuweisung
VPN IP-Netze
Zertifikats-Überprüfung
Firewall-Einstellungen

Je nachdem, welcher Begriff markiert wird, zeigt sich das entsprechende Feld mit den zugehörigen Parametern (siehe → 4. Konfigurationsparameter).

Ok – Profil

Die Konfiguration eines Profils ist abgeschlossen, wenn Sie das Konfigurationsfenster mit “OK” schließen. Das neue oder geänderte Profil ist im Monitor sofort verfügbar. Es kann im Monitor über die Profilauswahl selektiert werden und über das Menü “Verbindung → Verbinden” sofort zur Anwahl an das Zielsystem verwendet werden.

Kopieren – Profil

Um die Parameter-Einstellungen eines bereits definierten Profils zu kopieren, markieren sie das zu kopierende Profil in der Liste und klicken Sie auf den Kopieren-Button. Daraufhin wird das Grundeinstellungen-Parameterfeld geöffnet. Ändern Sie nun den Eintrag in “Profil-Name” und klicken Sie anschließend Ok. Nur wenn Sie den Namen des Profils ändern, kann es auch als neuer Eintrag in der Liste der Profile vermerkt werden.

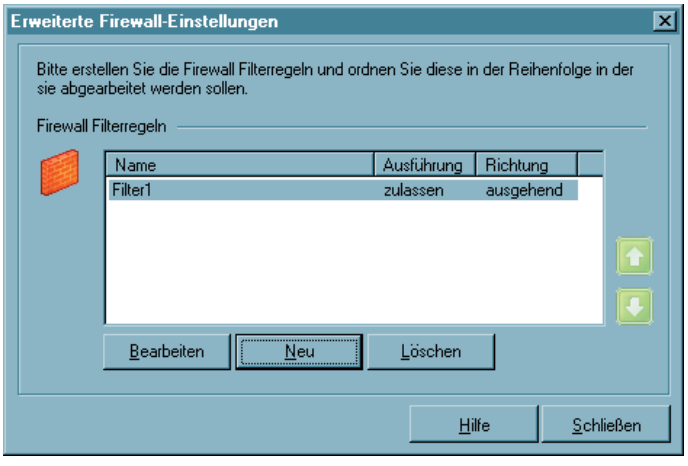
Ein kopiertes Profil muss einen neuen, noch nicht vergebenen, Namen erhalten. Nur so kann es in der Liste der Profile abgelegt werden.

Löschen – Profil

Um ein Profil zu löschen, wählen Sie es aus und klicken den Löschen-Button.

Erweiterte Firewall-Einstellungen

Mit diesem Filter-Editor können Filter für ein- und ausgehenden Datenverkehr definiert werden. Die Filter können für Protokolle, Netzwerk- und Host-IP-Adressen gesetzt werden.



Nachdem Sie den Menüpunkt gewählt haben, erscheint im ersten Fenster eine Liste der Firewall-Filterregeln. Jede Regel hat einen frei zu vergebenden Namen, die Ausführung der Filterregel kann zugelassen oder abgelehnt werden und die Richtung kann als ausgehend oder eingehend definiert werden.

Mit den grünen Pfeiltasten kann die Reihenfolge der Filterregeln festgelegt weden.

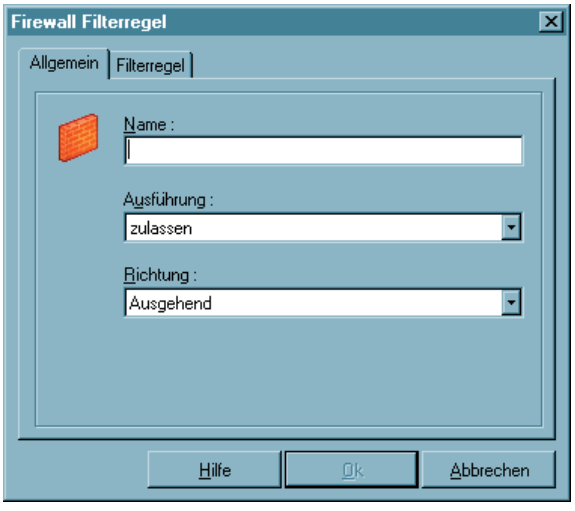
Die Buttons “Bearbeiten”, “Neu” und “Löschen” beziehen sich auf die jeweils markierte Filterregel.

Beachten Sie bitte, dass eine gelöschte Filterregel nicht wieder hergestellt werden kann.

Mit den Buttons “Neu” und “Bearbeiten” öffnen sich weitere Fenster zur Definition der Filter:

– Allgemein | Firewall
– Filterregel | Firewall

Allgemein | Firewall



Name | Firewall

Geben Sie einen Namen für die zu definierende Filterregel ein.

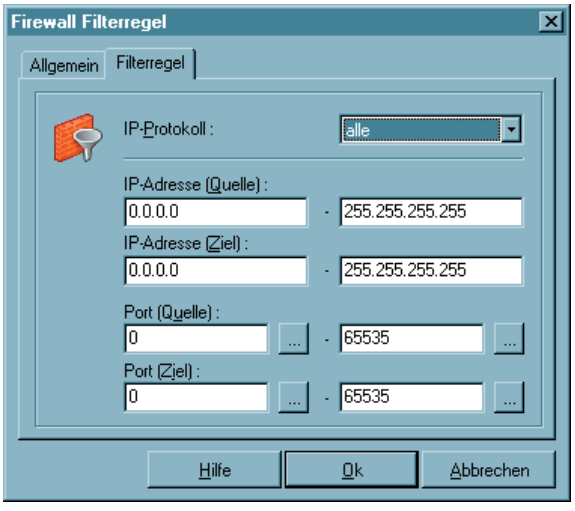
Ausführung | Firewall

aus	=	mit diesem Befehl wird die Filterregel inaktiviert; damit ist es nicht nötig sie zu löschen
ablehnen	=	alle IP-Pakete mit Adressen aus dem definierten Bereich werden verworfen
zulassen	=	IP-Pakete mit Adressen aus dem definierten Bereich werden für den Datenverkehr zugelassen

Richtung | Firewall

eingehend	=	die Filterregel gilt für eingehende IP-Pakate
ausgehend	=	die Filterregel gilt für ausgehende IP-Pakate

Filterregel | Firewall



In diesem Fenster kann bestimmt werden, für welches Protokoll die Filterregel gelten soll, für welchen IP-Adressen-Bereich und für welchen Port-Adressen-Bereich.

IP-Protokoll | Firewall

Hier wird bestimmt, für welches Transport-Protokoll diese Regel gelten soll, ICMP, TCP, oder UDP. Eines dieser angebotenen Protokolle oder alle können gewählt werden.

IP-Adresse (Quelle) | Firewall

Dies kann eine Host-IP-Adresse oder ein Adress-Bereich sein.

IP-Adresse (Ziel) | Firewall

Dies kann eine Host-IP-Adresse oder ein Adress-Bereich sein.

Port (Quelle) | Firewall

Dies kann entweder eine individuelle TCP- oder UDP-Portnummer sein oder ein Bereich von Portnummern. Bestimmen Sie die Portnummern mit den zugeteilten Diensten indem Sie den Auswahl-Button [...] drücken.

Port (Ziel) | Firewall

Dies kann entweder eine individuelle TCP- oder UDP-Portnummer sein oder ein Bereich von Portnummern. Bestimmen Sie die Portnummern mit den zugeteilten Diensten, indem Sie den Auswahl-Button [...] drücken.

Amtsholung

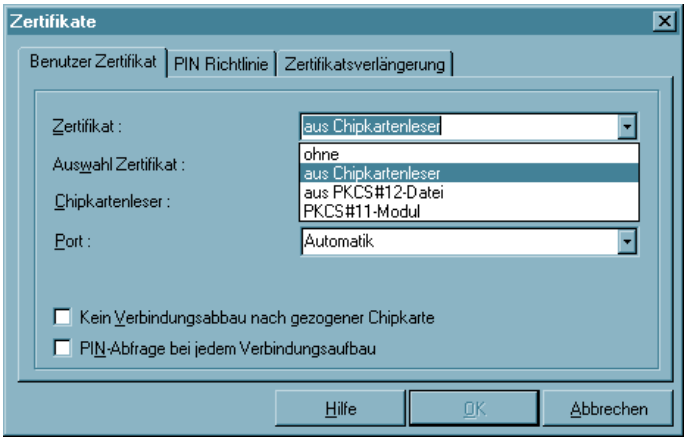
Eine Amtsholung ist dann nötig, wenn der IPSec Client an einer Nebenstellenanlage betrieben wird. Damit die definierten Profile des IPSec Clients auch im mobilen Einsatz verwendbar bleiben, ohne Rufnummern umkonfigurieren zu müssen, kann, sofern an einem Anschluss eine Amtsholung nötig wird, diese hier eingetragen werden. Die Nummer für die Amtsholung wird dann für alle Zielrufnummern der Profile automatisch mitgewählt.

Benutzer-Zertifikat | Konfiguration

Klicken Sie auf die Menüabzweigung “Konfiguration – Zertifikate”, so können Sie zunächst bestimmen, ob Sie die Zertifikate und damit die “Erweiterte Authentisierung” nutzen wollen, und wo Sie die Benutzer-Zertifikate hinterlegen wollen.

In weiteren Konfigurationsfeldern werden die Richtlinien zur PIN-Eingabe festgelegt und das Zeitintervall eingestellt innerhalb dessen das Zertifikat abläuft bzw. eine Zertifikatsverlängerung beantragt werden muss.

Zertifikat



ohne: Wählen Sie in der Listbox “Zertifikat” die Einstellung “ohne”, so wird kein Zertifikat ausgewertet und die “Erweiterte Authentisierung” findet nicht statt.

aus Chipkartenleser: Wählen Sie “aus Chipkartenleser” in der Listbox, so werden bei der “Erweiterten Authentisierung” die relevanten Zertifikate von der Smart Card in ihrem Chipkartenleser ausgelesen.

aus PKCS#12-Datei: Wählen Sie “aus PKCS#12-Datei” aus der Listbox, so werden bei der “Erweiterten Authentisierung” die relevanten Zertifikate aus einer Datei auf der Festpplatte Ihres Rechners gelesen.

PKCS#11-Modul: Wählen Sie “PKCS#11-Modul” in der Listbox, so werden bei der “Erweiterten Authentisierung” die relevanten Zertifikate von der Smart Card in einem Chipkartenleser oder von einem Token gelesen.

Chipkartenleser

Wenn Sie die Zertifikate von der Smart Card mit Ihrem Lesegerät nutzen wollen, wählen Sie Ihren Chipkartenleser aus der Listbox. (Siehe auch → PIN eingeben)

Chipkartenleser (PC/SC-konform)
Die Client Software unterstützt automatisch alle Chipkartenleser, die PC/SC-konform sind. Die Client Software erkennt dann den Chipkartenleser nach einem Boot-Vorgang automatisch. Erst dann kann der installierte Leser ausgewählt und genutzt werden.

Chipkartenleser (CT-API-konform)
Mit der aktuellen Software werden Treiber für die Modelle SCM Swapsmart und SCM 1x0 (PIN Pad Reader) mitgeliefert. Sollte der Chipkartenleser mit den mitgelieferten Treibern nicht funktionieren oder ein anderer Chipkartenleser installiert sein, wenden Sie sich unbedingt an den Hersteller. Nehmen Sie außerdem folgende Einstellung in der Client Software vor: Editieren Sie die Datei NCPPKI.CONF, befindlich im Windows\System-Verzeichnis (unter Windows 95/98) oder System32-Verzeichnis (unter Windows NT/2000) mit einem ASCII-Editor, indem Sie als “ReaderName” den Namen des angeschlossenen Chipkartenlesers (xyz) eintragen und als DLLWIN95 bzw. DLLWINNT den Namen des installierten Treibers eintragen. (Der Standardname für CT-API-konforme Treiber ist CT32.DLL).

Wichtig: Nur die Treiber sind in der Liste sichtbar, die mit “visible = 1" auf sichtbar gesetzt wurden!

```
ReaderName = SCM Swapsmart (CT-API) -> xyz
DLLWIN95   = scm20098.dll           -> ct32.dll
DLLWINNT   = scm200nt.dll           -> ct32.dll
```

Nach einem Boot-Vorgang erscheint der “ReaderName” im Monitor-Menü.

Port

Der Port wird bei korrekter Installation des Lesegeräts automatisch bestimmt. Bei Unstimmigkeiten können die COM Ports 1-4 gezielt angesteuert werden.

Auswahl Zertifikat

1. Zertifikat ... 3.: (Standard = 1) Aus der Listbox kann aus bis zu drei verschiedenen Zertifikaten gewählt werden, die sich auf der Chipkarte befinden. Die Anzahl der Zertifikate auf der Chipkarte ist abhängig von der Registration Authority, die diese Karte brennt. Wenden Sie sich zu weiteren Fragen bitte an Ihren Systemadministrator.

Auf den Chipkarten von Signtrust und NetKey 2000 befinden sich drei Zertifikate:
(1) zum Siginieren
(2) zum Ver- und Entschlüsseln
(3) zum Authentisieren (optional bei NetKey 2000)

PKCS#12-Dateiname

Nutzen Sie das PKCS#12-Format, so erhalten Sie von Ihrem Systemadministrator eine Datei, die auf der Festplatte Ihres Rechners eingespielt werden muss. In diesem Fall muss Pfad und Dateiname der PKCS#12-Datei eingegeben, bzw. nach einem Klick auf den [...]-Button (Auswahl-Button) die Datei ausgewählt werden.

Statt den Verzeichnisnamen komplett einzugeben, kann der Name dynamisch zusammengesetzt werden. Z.B.:

```
%SYSTEMRROT%\ncple\user1.p12
%SYSTEMDRIVE%\winxxx\ncple\user1.p12
```

Wichtig: Die Strings für den Dateinamen können mit Variablen eingegeben werden. Dies erleichtert insbesondere das Handling der Konfigurationsdateien mit dem Client Manager, da nun für alle Benutzer die gleichen Strings mit Umgebungsvariablen eingegeben werden können.

PKCS#11-Modul

Nutzen Sie das PKCS#11-Format, so erhalten Sie eine DLL vom Hersteller des Chipkartenlesers oder des Tokens, die auf der Festplatte Ihres Rechners eingespielt werden muss. In diesem Fall muss Pfad und Dateiname des Treibers eingegeben werden. Statt den Verzeichnisnamen für die PKCS#11.DLL komplett einzugeben, kann der Name dynamisch zusammengesetzt werden. Z.B.:

```
%SYSTEMRROT%\ncple\pkcs#11.dll
%SYSTEMDRIVE%\winxxx\ncple\ pkcs#11.dll
```

Wichtig: Die Strings für das Modul können mit Variablen eingegeben werden. Dies erleichtert insbesondere das Handling der Konfigurationsdateien mit dem Client Manager, da nun für alle Benutzer die gleichen Strings mit Umgebungsvariablen eingegeben werden können.

Kein Verbindungsabbau bei gezogener Chipkarte

Beim Ziehen der Chipkarte wird nicht unbedingt die Verbindung abgebaut. Damit “Kein Verbindungsabbau bei gezogener Chipkarte” erfolgt, muss diese Funktion aktiviert werden.

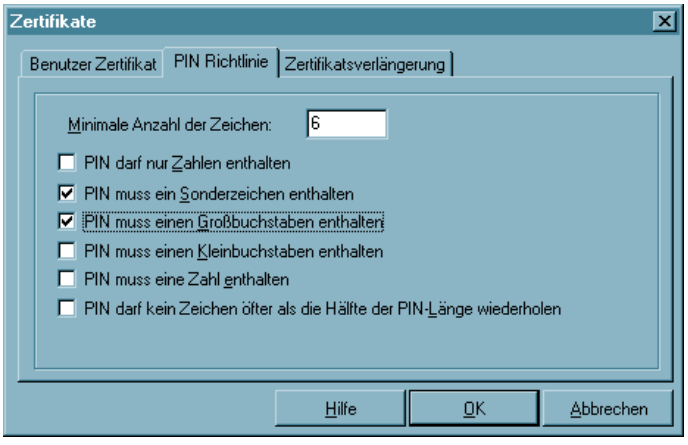
PIN-Abfrage bei jedem Verbindungsaufbau

Standardeinstellung: Wird diese Funktion nicht genutzt, so wird die PIN nur einmalig beim ersten Verbindungsaufbau des IPSec Clients abgefragt.

Wird diese Funktion aktiviert, so wird bei jedem Verbindungsaufbau die PIN erneut abgefragt.

Wichtig: Ist der Monitor nicht gestartet, kann kein PIN-Dialog erfolgen. In diesem Fall wird bei einem automatischen Verbindungsaufbau die Verbindung ohne erneute PIN-Eingabe hergestellt!

PIN-Richtlinie



Für die PIN können Richtlinien festgelegt werden, die bei Eingabe oder Änderung der PIN beachtet werden müssen.

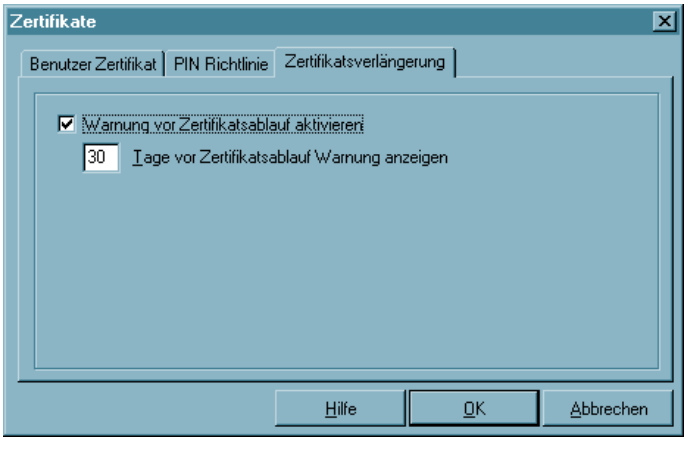
Minimale Anzahl der Zeichen

Standard ist eine 6-stellige PIN. Aus Sicherheitsgründen werden 8 Stellen empfohlen.

Weitere Richtlinien

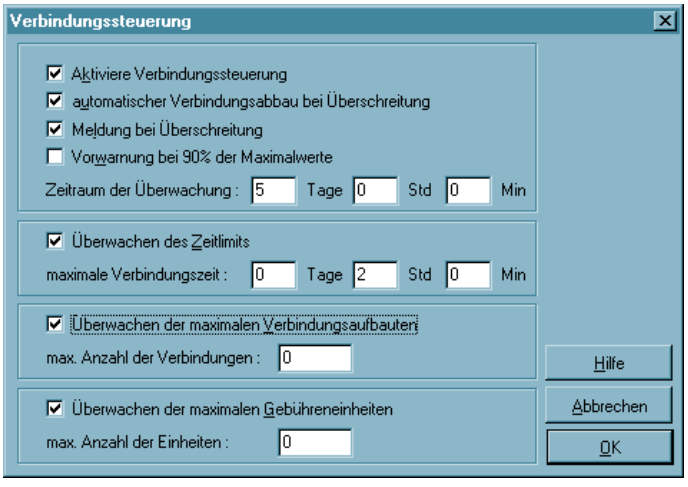
Es wird empfohlen alle PIN-Richtlinien einzusetzen, außer der, dass nur Zahlen enthalten sein dürfen. Zudem sollte die PIN nicht mit einer Zahl beginnen. Die vorgegebenen Richtlinien werden eingeblendet, wenn die PIN geändert wird und die Richtlinien, die bei der Eingabe erfüllt werden, werden grün markiert (siehe → PIN ändern).

Zertifikatsverlängerung



In diesem Konfigurationsfeld kann eingestellt werden, ob und wie viele Tage vor Ablauf der Gültigkeit des Zertifikats eine Meldung ausgegeben werden soll, die vor dem Ablauf der Gültigkeit warnt. Sobald die eingestellte Zeitspanne vor Ablauf in Kraft tritt, wird bei jeder Zertifikatsverwendung eine Meldung aufgeblendet, die auf das Ablaufdatum des Zertifikats hinweist.

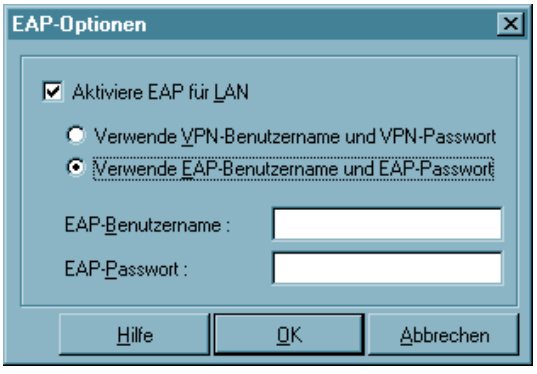
Verbindungssteuerung



Die "Verbindungssteuerung Einstellungen" bewirken eine automatische Überwachung. So können Sie wählen, welche der Limits Sie sich für Ihre Kommunikation setzen (Überwachen des Zeitlimits, der maximalen Verbindungsaufbauten und/oder der maximalen Gebühreneinheiten), für welchen Zeitraum diese Limits gültig sein sollen (Zeitraum der Überwachung) und wie Sie von Limit-Überschreitungen in Kenntnis gesetzt werden möchten (Meldung und Vorwarnung), oder ob ein automatischer Verbindungsabbau stattfinden soll.

Wenn ein von Ihnen definiertes Limit überschritten wurde, wird jede weitere Kommunikation unterbunden, bis Sie die "Sperre" wieder aufgehoben haben (siehe → Sperre aufheben).

EAP-Optionen



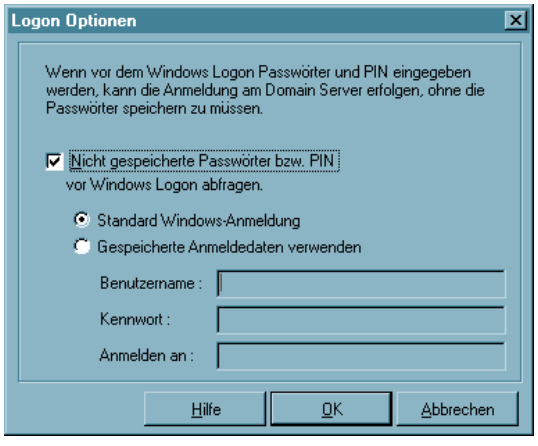
Der Einsatz des Extensible Authentication Protocols Message Digest5 (EAP MP5) kann über das Hauptmenü des Monitors unter "Konfiguration – EAP-Optionen" eingestellt werden. Dieses Protokoll kann dann zum Einsatz kommen, wenn für den Zugang zum LAN ein Switch oder für das wireless LAN ein Access Point verwendet werden, die 802.1x-fähig sind und eine entsprechende Authentisierung unterstützen.

Mit dem Extensible Authentication Protocol (EAP MP5) kann verhindert werden, dass sich unberechtigte Benutzer über die Hardware-Schnittstelle in das LAN einklinken.

Zur Authentisierung kann wahlweise "Benutzername" mit "Passwort" (aus dem Konfigurationsfeld "Identität") verwendet werden oder ein eigener "EAP-Benutzername" mit einem "EAP-Passwort".

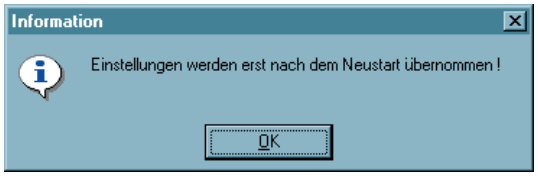
■ Logon-Optionen

Diese Funktion kann nur unter Windows NT/2000 und Windows XP genutzt werden.



Wenn Sie diesen Menüpunkt mit einem Mausklick wählen, können Sie im folgenden Fenster entscheiden, ob vor dem Windows-Logon an einer remote Domain die Verbindung von der Client-Software zum Network Access Server aufgebaut werden soll. Dies bedeutet, dass die Client-Software beim nächsten Booten die Verbindung aufbaut. Für diesen Verbindungsaufbau müssen Sie gegebenenfalls die PIN für Ihr Zertifikat und das (nicht gespeicherte) Passwort für die Client-Software eingeben.

Nachdem die Verbindung zum Network Access Server von der Client-Software hergestellt wurde, können Sie sich an der remote Domain anmelden. Diese Anmeldung erfolgt dann bereits verschlüsselt.



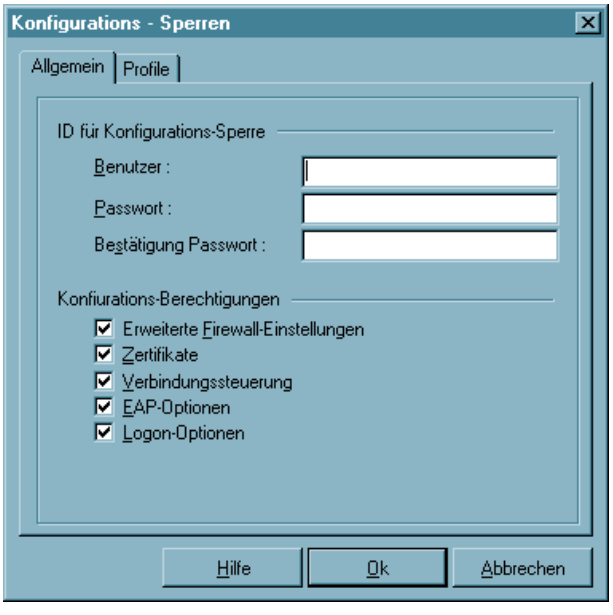
Nach jeder Änderung der “Logon Optionen” muss der Rechner gebootet werden.

Konfigurations-Sperren

Über die Konfigurations-Sperren kann das Konfigurations-Hauptmenü im Monitor so modifiziert werden, dass der Benutzer die voreingestellten Konfigurationen nicht mehr abändern kann, bzw. ausgewählte Parameterfelder für den Benutzer nicht sichtbar sind.

Die Konfigurations-Sperren werden in der definierten Form erst wirksam, wenn die Einstellungen mit “OK” übernommen werden. Wird der “Abbrechen”-Button gedrückt, wird auf die Standard-Einstellung zurückgesetzt.

Allgemein | Konfigurations-Sperren



Um die Konfigurations-Sperren wirksam festlegen zu können, muss eine ID eingegeben werden, die sich aus “Benutzer” und “Passwort” zusammensetzt. Das Passwort muss anschließend bestätigt werden.

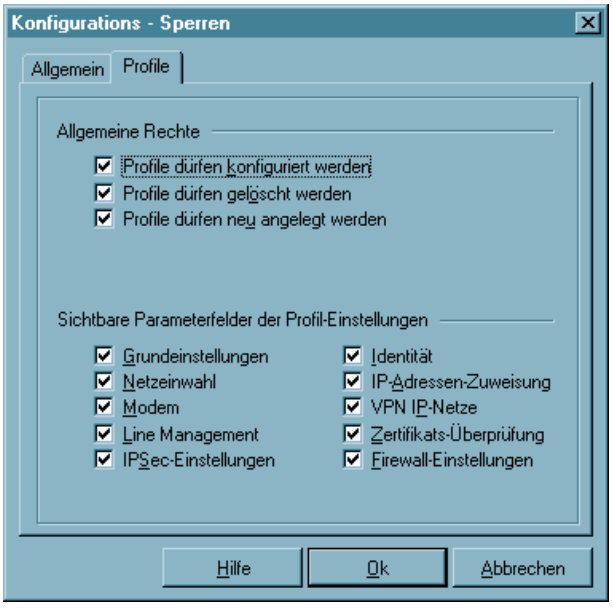
Bitte beachten Sie, dass die ID für die Konfigurations-Sperre unbedingt nötig ist, die Sperren wirksam werden zu lassen oder die Konfigurations-Sperren auch wieder aufzuheben. Wird die ID vergessen, besteht keine Möglichkeit mehr, die Sperren wieder aufzuheben!

Anschließend kann die Berechtigung, die Menüpunkte unter dem Hauptmenüpunkt “Konfiguration” zu öffnen, für den Benutzer eingeschränkt werden. Standardmäßig kann der Benutzer alle Menüpunkte öffnen und die Konfigurationen bearbeiten. Wird zu einem Menüpunkt der zugehörige Haken mit einem Mausklick entfernt, so kann der Benutzer diesen Menüpunkt nicht mehr öffnen.

Profile | Konfigurations-Sperren

Die Bearbeitungsrechte für die Parameter in den Profil-Einstellungen sind in zwei Sparten unterteilt:

– Allgemeine Rechte
– Sichtbare Parameterfelder der Profile



Allgemeine Rechte

Die allgemeinen Rechte beziehen sich nur auf die (Konfiguration der) Profile. Wird festgelegt “Profile dürfen neu angelegt werden”, “Profile dürfen konfiguriert werden” bleibt jedoch ausgeschlossen, so können zwar mit dem Assistenten neue Profile definiert werden, eine nachfolgende Änderung einzelner Parameter ist dann jedoch nicht mehr möglich.

Sichtbare Parameterfelder der Profile

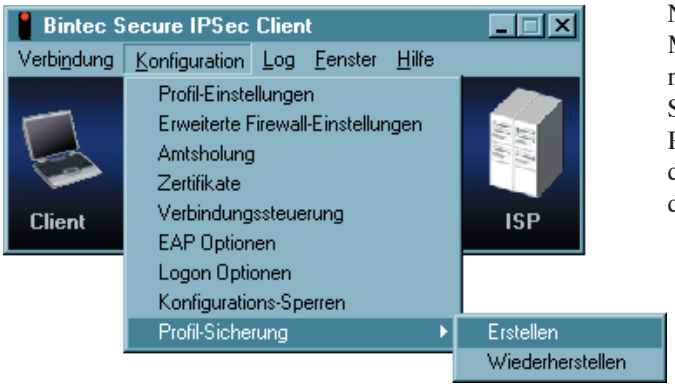
Die Parameterfelder der Profil-Einstellungen können für den Benutzer ausgeblendet werden.

Beachten Sie, dass Parameter eines nicht sichtbaren Feldes auch nicht konfiguriert werden können.

Profil-Sicherung

Existiert noch kein gesichertes Profil, zum Beispiel bei einer Erstinstallation, so wird automatisch ein erstes angelegt (NCPPHONE.SAV).

Erstellen



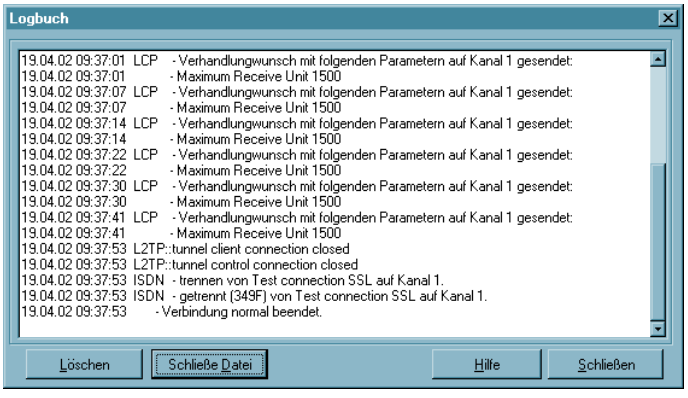
Nach jedem Klick auf den Menüpunkt “Erstellen” wird nach einer Sicherheitsabfrage eine Profil-Sicherung angelegt, die die Konfiguration zu diesem Zeitpunkt enthält.

Wiederherstellen

Nach jedem Klick auf “Wiederherstellen” wird die letzte Profil-Sicherung eingelesen. Änderungen in der Konfiguration, die seit der letzten Profil-Sicherung vorgenommen wurden gehen damit verloren.

3.2.3 Log

Mit der Log-Funktion werden die Kommunikationsereignisse der IPSec Client Software mitprotokolliert. Wählen Sie die Log-Funktion an, öffnet sich das Fenster des “Logbuches”.



Die hier abgebildeten Daten werden bis zum nächsten Reboot im Speicher gehalten.

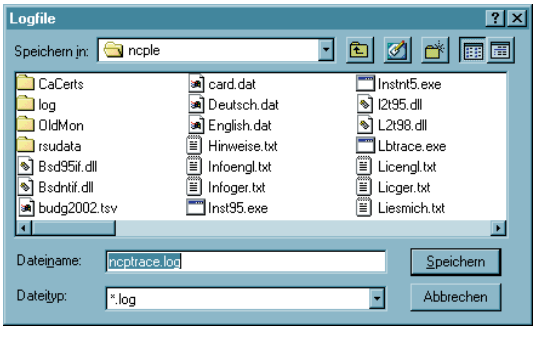
Eine zusätzliche Log-Datei speichert die Aktionen des Clients selbständig für die letzten sieben Tage. Log-Ausgaben, die älter als sieben Betriebstage sind, werden automatisch gelöscht. Die Datei steht unter NCPLE\LOG und heißt NCPyymmdd.LOG. Sie wird mit Datumsangabe (yymmdd) immer bei Beenden des Monitors geschrieben. Die Datei kann mit einem Texteditor geöffnet und analysiert werden.

■ Logbuch

Die Buttons des Logbuchfensters haben folgende Funktionen:

– Öffne Datei
– Schließe Datei
– Löschen – Fensterinhalt
– Schließen – Log-Fenster

Öffne Datei



Wenn Sie auf diesen Button klicken, erhalten Sie in einem weiteren Fenster die Möglichkeit Name und Pfad einer Datei einzugeben, in die der Inhalt des Log-Fensters geschrieben wird (Standard: ncptrace.log).

Alle Transaktionen mit der IPSec Client Software, wie Anwahl und Empfang, einschließlich der Rufnummern, werden automatisch mitprotokolliert und in diese Datei geschrieben, bis Sie auf den Button mit “Schließe Datei” klicken. Wenn Sie eine Log-Datei anlegen, können Sie die Transaktionen mit dem IPSec Client über einen längeren Zeitraum verfolgen.

Schließe Datei

Wenn Sie auf diesen Button klicken, wird die Datei geschlossen, die Sie mit “Öffne Datei” angelegt haben. Die geschlossene Log-Datei kann zur Analyse der Transaktionen mit dem IPSec Client oder zur Fehlersuche verwendet werden.

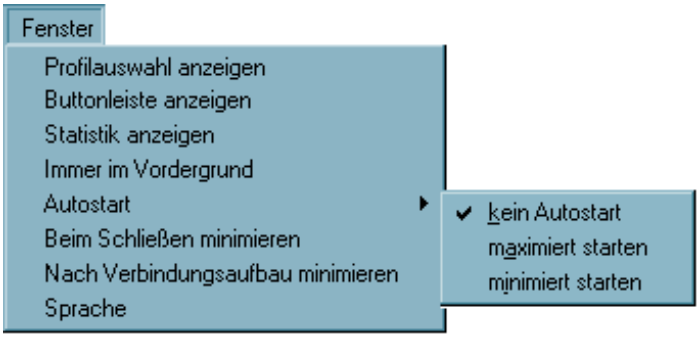
Löschen – Fensterinhalt

Wenn Sie auf diesen Button drücken wird der Inhalt des Log-Fensters gelöscht.

Schließen – Log-Fenster

Wenn Sie auf “Schließen” klicken, schließen Sie das Fenster des “Logbuches” und kehren zum Monitor zurück.

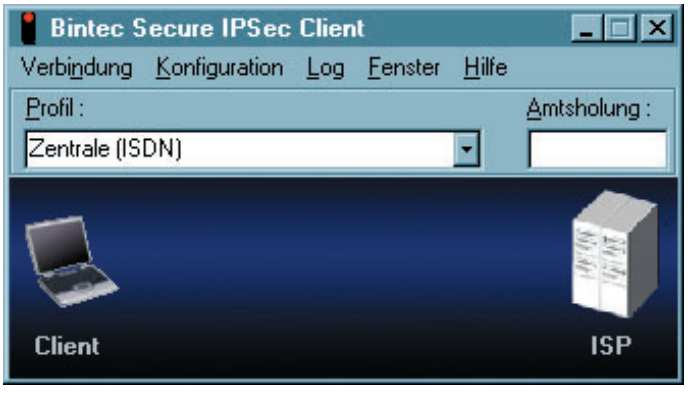
3.2.4 Fenster



Unter dem Menüpunkt “Fenster” können Sie die Bedienoberfläche des Monitors variieren und die Sprache für die Monitoroberfläche festlegen.

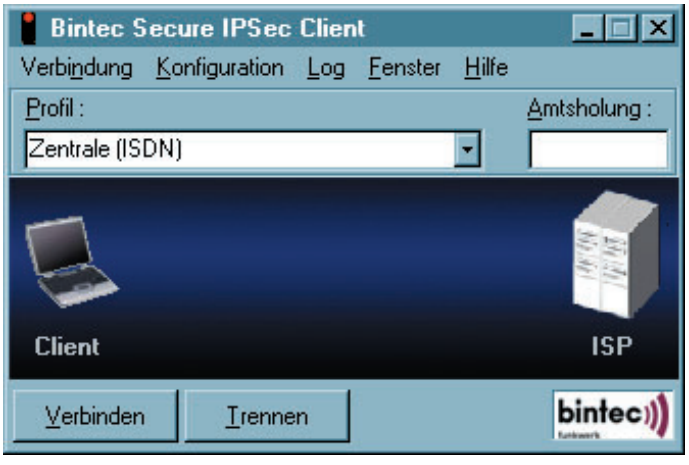
■ **Profilauswahl anzeigen**

Links: Minimierte Darstellung



Wenn Sie auf “Profilauswahl anzeigen” klicken, kann aus der Liste der konfigurierten Profile das gewünschte ausgewählt werden (Bild unten).

Buttonleiste anzeigen



Wenn Sie auf "Buttonleiste anzeigen" klicken, werden Buttons für die Menüpunkte "Verbinden" und "Trennen" aus dem Hauptmenü "Verbindung" eingeblendet.

Statistik anzeigen

Wenn Sie auf "Statistik anzeigen" klicken, werden Informationen zu Datenmenge, Verbindungszeit, Timeout etc. angezeigt. Die Monitor-Oberfläche ist dann entsprechend größer.

Immer im Vordergrund

Wenn Sie "Immer im Vordergrund" geklickt haben, wird der Monitor immer im Bildschirmvordergrund angezeigt, unabhängig von der jeweils aktiven Anwendung.

■ Autostart

Mit diesem Menüpunkt wird der Monitor so eingestellt, dass er nach dem Booten selbständig startet. “Autostart” ersetzt den Menüpunkt “Fenster – Nach Booten starten”. Über den neuen Menüpunkt können folgende Optionen eingestellt werden:

- ☐ kein Autostart: nach dem Booten nicht automatisch starten
- ☐ minimiert starten: nach dem Booten den Monitor starten und minimiert darstellen
- ☐ maximiert starten: nach dem Booten den Monitor starten und in normaler Größe darstellen

Wenn Sie oft mit der IPSec Client Software arbeiten und die Informationen des Monitors benötigen, so sollten Sie die Einstellung “maximiert starten” wählen. Prinzipiell ist es für die Kommunikation mit dem Zielsystem nicht nötig, den Monitor zu starten.

■ Beim Schließen minimieren

Wird der Monitor bei einer bestehenden Verbindung über den Schließen-Button [x] rechts in der Kopfzeile oder das Systemmenü links in der Kopfzeile geschlossen [Alt + F4], so informiert ein Meldungsfenster darüber, dass kein Ampelsymbol (Tray Icon) mehr in der Task-Leiste erscheint, worüber der Status dieser Verbindung kontrolliert werden könnte, d.h. der Benutzer kann dann auf der Oberfläche seines Desktops nicht erkennen, ob und wie lange noch Verbindungsgebühren anfallen, oder ob die Verbindung bereits beendet wurde.

(Um in diesem Fall den Status der Verbindung zu erfahren und sie gegebenenfalls korrekt zu beenden, muss der Monitor erneut gestartet werden.)

Ist dieser Menüpunkt aktiviert, so wird der Monitor beim Schließen über den Button [x] rechts in der Kopfzeile oder über [Alt + F4] nur minimiert und erscheint als Ampelsymbol in der Task-Leiste, worüber der Status der Verbindung abgelesen werden kann. Der Klick auf den Schließen-Button [x] der Kopfzeile hat in dieser Einstellung die gleiche Wirkung wie der Klick auf den Minimieren-Button [-] der Kopfzeile.

(In der Darstellung des Ampelsymbols in der Task-Leiste kann nach einem rechten Mausklick auf das Symbol das mögliche Zielsystem abgelesen und die Verbindung aufgebaut oder getrennt werden, bzw. bei abgebauter Verbindung der Monitor auch beendet werden.)

Das Beenden des Monitors ist nur noch über das Hauptmenü “Verbindung – Beenden” möglich.

- **Nach Verbindungsaufbau minimieren**

  Ist dieser Menüpunkt aktiviert, so wird der Monitor nach erfolgreichem Verbindungsaufbau automatisch minimiert, nicht jedoch beendet.

Das Beenden des Monitors ist nur über das Hauptmenü “Verbindung – Beenden” möglich.

- **Sprache**

  Die IPSec Client Software ist mehrsprachig angelegt. Die Standardsprache bei Auslieferung ist Deutsch. Um eine andere Sprache zu wählen, klicken Sie “Language / Sprache” im Pulldown-Menü Fenster und wählen die gewünschte Sprache.

3.2.5 Hilfe

Die “Hilfe” zeigt Ihnen den kompletten Hilfetext mit Inhaltsverzeichnis und Index.

Unter dem Menüpunkt Hilfe finden Sie mit Klick auf “Info” die Versionsnummer Ihrer eingesetzten Software und Treiber.

4. Konfigurationsparameter

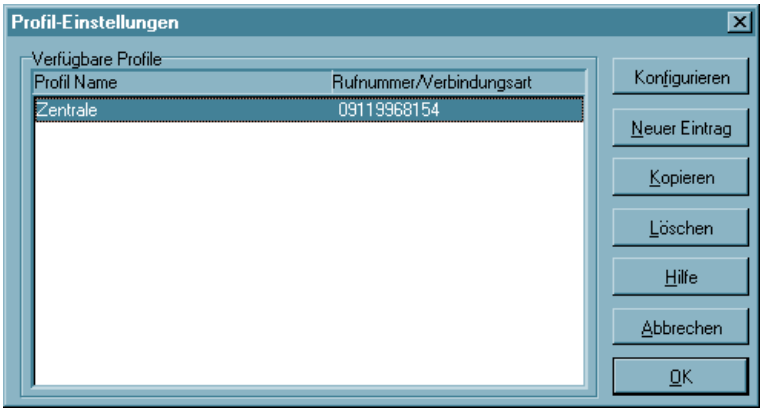
Die IPSec Client Software gestattet die Einrichtung individueller Profile für entsprechende Zielsysteme, die nach den Benutzeranforderungen konfiguriert werden können.

Im folgenden sind alle Parameterbeschreibungen aufgeführt, und sie sind so angeordnet, wie sie auf der Oberfläche des Client Monitors erscheinen.

Um die Einstellungen Ihres IPSec Clients auf Funktionstüchtigkeit hin zu überprüfen, bietet Bintec einen entsprechenden öffentlichen Testzugang. Eine detaillierte Konfigurationsanleitung zur Nutzung dieses VPN-Testzugangs in Verbindung mit dem Bintec Secure IPSec Client finden Sie unter www.bintec.de.

4.1 Profil-Einstellungen

Nachdem Sie “Profil-Einstellungen” im Menü des Monitors angeklickt haben, öffnet sich das Menü und zeigt eine Übersicht über die bereits definierten Profile und die Rufnummern der zugehörigen Ziele.



Seitlich finden Sie Buttons, über die Sie die Einträge des Telefonbuchs (Zielsysteme) modifizieren können.

Um ein neues Profil zu definieren, klicken Sie in der Menüleiste des Monitors auf “Profil-Einstellungen”. Das Menü öffnet sich nun und zeigt die bereits definierten Profile. Klicken Sie jetzt auf “Neuer Eintrag”. Jetzt legt der “Assistent für ein neues Profil” mit Ihrer Hilfe ein neues an. Dazu blendet er die unbedingt notwendigen Parameter auf. Wenn Sie die Einträge in diesen Feldern vorgenommen haben, ist ein neues Profil angelegt. Für alle weiteren Parameterfelder werden Standardwerte eingetragen.

Um diese Standardwerte zu editieren, d.h. weitere Parameter so einzustellen, wie es den Verbindungsanforderungen zum zugehörigen Zielsystem entspricht, wählen Sie mit der Maus das Profil aus, dessen Werte Sie ändern möchten und klicken anschließend auf “Konfigurieren”.

Um die Definitionen eines bereits definierten Profils zu kopieren, klicken Sie “Kopieren”.

Um ein Profil zu löschen, wählen Sie es aus und klicken “Löschen”.

Parameterfelder:

Die Parameter, die die jeweilige Verbindung über das Profil zu den Zielen spezifizieren, sind in verschiedenen Parameterfeldern gesammelt. In der Kopfzeile steht der Name des Profils (siehe auch → Profil-Einstellungen, Konfigurieren). Seitlich sind die Titel der Parameterfelder angeordnet:

1 ***Grundeinstellungen***

2 ***Netzeinwahl***

3 ***Modem***

4 ***Line Management***

5 ***IPSec-Einstellungen***

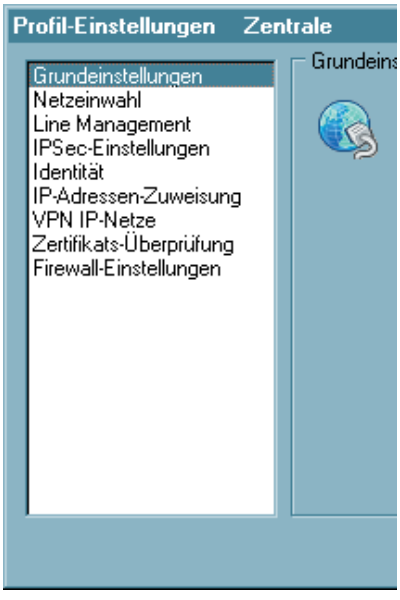
6 ***Identität***

7 ***IP-Adressen-Zuweisung***

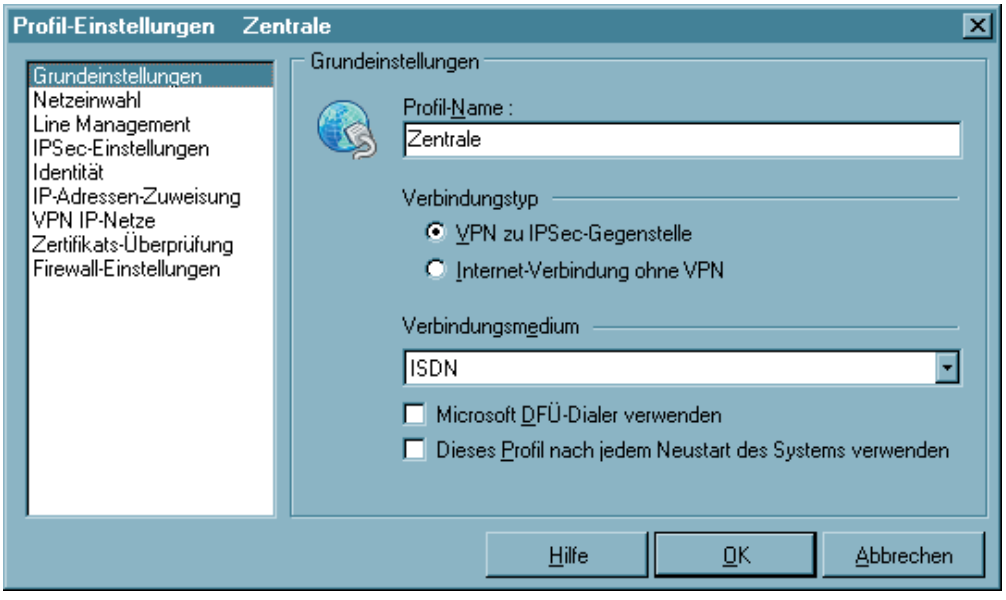
8 ***VPN IP-Netze***

9 ***Zertifikats-Überprüfung***

10 ***Firewall-Einstellungen***



4.1.1 Grundeinstellungen



Im Parameterfeld “Grundeinstellungen” wird der “Profil-Name”, den “Verbindungstyp” und das “Verbindungsmedium” zu einem Profil eingegeben.

Parameter:

- ☐ Profil-Name
- ☐ Verbindungstyp
- ☐ Verbindungsmedium
- ☐ Microsoft DFÜ-Dialer verwenden
- ☐ Dieses Profil nach jedem Neustart des Systems verwenden

Profil-Name

Wenn Sie ein neues Profil definieren, sollten Sie zunächst einen unverwechselbaren Namen für dieses System eintragen (z.B. IBM London). Der Name des Profils darf jeden gewünschten Buchstaben wie auch Ziffern beinhalten und darf, Leerzeichen mitgezählt, bis zu 39 Zeichen lang sein.

Verbindungstyp

Alternativ stehen mit dem IPSec Client zwei Verbindungstypen zur Wahl:

VPN zu IPSec-Gegenstelle:

In diesem Fall wählen Sie sich mit dem IPSec Client in das Firmennetz ein (bzw. an das Gateway an). Dazu wird ein VPN-Tunnel aufgebaut.

Internet-Verbindung ohne VPN:

In diesem Fall nutzen Sie den IPSec Client nur zur Einwahl in das Internet. Dabei wird Network Address Translation (IPNAT) weiterhin im Hintergrund genutzt, sodass nur Datenpakete akzeptiert werden, die angefordert wurden.

Verbindungsmedium

Die Verbindungsart kann für jedes Profil eigens eingestellt werden, vorausgesetzt Sie haben die entsprechende Hardware angeschlossen und in Ihrem (Windows-)System installiert.

ISDN:

Angeschlossene Hardware: ISDN-Hardware mit Capi 2.0-Unterstützung;
Netze: ISDN-Festnetz;
Gegenstellen: ISDN-Hardware;

Modem:

Angeschlossene Hardware: Asynchrone Modems (PCMCIA-Modem, GSM-Karte) mit Com Port-Unterstützung;
Netze: Analoges Fernsprechnetz (PSTN) (auch GSM);
Gegenstellen: Modem oder ISDN-Karte mit digitalem Modem;

LAN (over IP):

Angeschlossene Hardware: LAN-Adapter;
Netze: Local Area Network mit Ethernet oder Token Ring;
Gegenstellen: Die Gegenstellen des lokalen Multiprotokoll-Routers im LAN;

xDSL (PPPoE):

Angeschlossene Hardware: Ethernet-Adapter, xDSL-Modem;
Netze: xDSL;
Gegenstellen: Access-Router im xDSL;

xDSL (AVM - PPP over CAPI):

Diese Verbindungsart kann gewählt werden, wenn eine AVM Fritz! DSL-Karte eingesetzt wird. Im Feld “Rufnummer (Ziel)” in der Gruppe “Netzeinwahl” können für die Verbindung über CAPI noch AVM-spezifische Intitialisierungskommandos eingetragen werden. Unter Windows Betriebssystemen wird jedoch empfohlen den Standard “xDSL (PPPoE)” zu verwenden, da damit direkt über die Netzwerkschnittstelle mit der Karte kommuniziert wird. Bei Verwendung der AVM Fritz! DSL-Karte wird keine separate zusätzliche Netzwerkkarte benötigt.

Netze: xDSL;
Gegenstellen: Access-Router im xDSL;

GPRS / UMTS:

Dieses Einwahlmedium wählen Sie, wenn die Einwahl über das Mobilfunknetz (GPRS oder UMTS) erfolgen soll. Beachten Sie dazu den Hinweis unter den Installationsvoraussetzungen zu “Analoges Modem”.

PPTP:

Microsoft Point-to-Point Tunnel Protocol;
Angeschlossene Hardware: Ethernet-Adapter, xDSL-Modem;
Netze: xDSL;
Gegenstellen: Access-Router im xDSL;

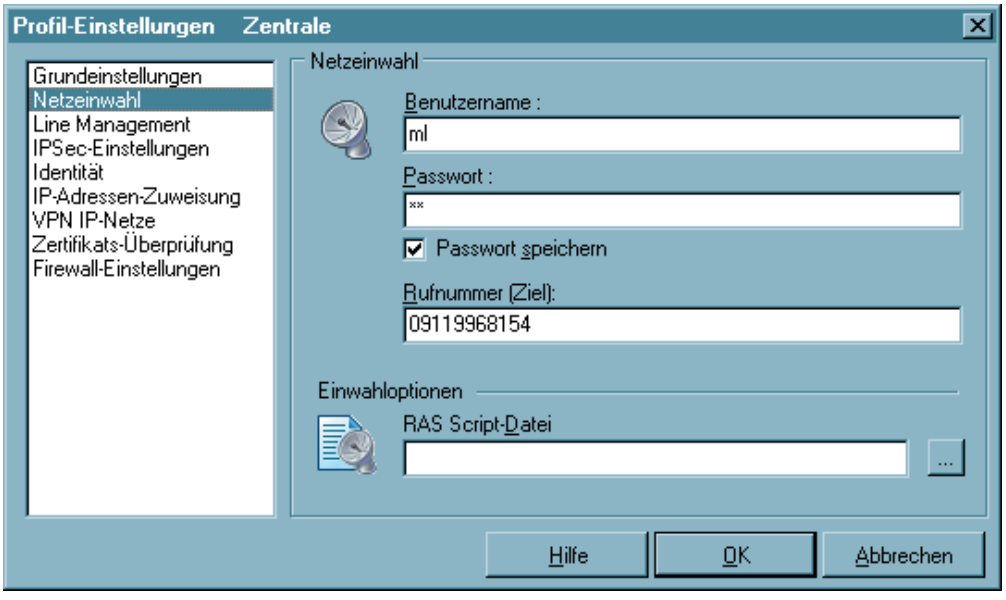
■ Microsoft DFÜ-Dialer verwenden

Zur Einwahl am ISP (Internet Service Provider) kann der Microsoft DFÜ-Dialer genutzt werden. Dies ist immer dann nötig, wenn der Einwahlpunkt ein Einwahl-Script benötigt. Der DFÜ-Dialer unterstützt dieses Script. Im Parameterfenster “Netzeinwahl” wird anschließend die Script-Datei unter Eingabe von Pfad und Namen zur eingespielten Script-Datei eingetragen (siehe → Script-Datei).

■ Dieses Profil nach jedem Neustart des Systems verwenden

Normalerweise wird der Client-Monitor nach einem Neustart mit dem zuletzt genutzten Profil geöffnet. Wird diese Funktion aktiviert, wird nach einem Neustart des Systems immer das hierzu gehörige Profil geladen, unabhängig davon, welches Profil zuletzt genutzt wurde.

4.1.2 Netzeinwahl



Dieses Parameterfeld beinhaltet den Benutzernamen und das Passwort, die bei der Anwahl an das Zielsystem zur Identifizierung benötigt werden. Diese beiden Größen werden auch für die PPP-Verhandlung zum ISP (Internet Service Provider) benötigt. Das Parameterfeld erscheint überhaupt nicht, wenn der IPSec Client mit dem Verbindungsmedium “LAN over IP” betrieben wird.

Parameter:

- ☐ Benutzername
- ☐ Passwort
- ☐ Passwort speichern
- ☐ Rufnummer (Ziel)
- ☐ Alternative Rufnummern
- ☐ Script-Datei

Benutzername

Mit dem “Benutzernamen” weisen Sie sich gegenüber dem Network Access Server (NAS) aus, wenn Sie eine Verbindung zum Zielsystem aufbauen wollen. Bei Kommunikation über das Internet benötigen Sie den Benutzernamen zur Identifikation am ISP (Internet Service Provider). Der Name für den Benutzer kann bis zu 254 Zeichen lang sein. Für gewöhnlich wird Ihnen ein “Benutzername” vom Zielsystem zugewiesen, da Sie vom Zielsystem (auch Radius- oder LDAP-Server) erkannt werden müssen. Sie erhalten ihn von Ihrem Stammhaus, vom Internet Service Provider oder dem Systemadministrator.

Passwort

Das Passwort benötigen Sie, um sich gegenüber dem Network Access Server (NAS) ausweisen zu können, wenn die Verbindung aufgebaut ist. Das Passwort darf bis zu 254 Zeichen lang sein. Für gewöhnlich wird Ihnen ein Passwort vom Zielsystem zugewiesen, da Sie vom Zielsystem auch erkannt werden müssen. Sie erhalten es von Ihrem Stammhaus, vom Internet Service Provider oder dem Systemadministrator.

Wenn Sie das Passwort eingeben, werden alle Zeichen als Stern (*) dargestellt, um sie vor ungewünschten Beobachtern zu verbergen. Es ist wichtig, dass Sie das Passwort genau nach der Vorgabe eintragen und dabei auch auf Groß- und Kleinschreibung achten.

Wird der Parameter “Passwort speichern” nicht aktiviert, so muss er bei jedem Verbindungsaufbau das Passwort per Hand eingeben.

Passwort speichern

Dieser Parameter muss aktiviert (angeklickt) werden, wenn gewünscht wird, dass das Passwort und das Passwort Ziel (sofern es eingegeben ist) gespeichert wird. Andernfalls werden die Passwörter gelöscht, sobald der PC gebootet wird oder ein Zielsystem gewechselt wird. Standard ist die aktivierte Funktion.

Wichtig: Bitte beachten Sie, dass im Falle gespeicherter Passwörter, jedermann mit Ihrer Client Software arbeiten kann – auch wenn er die Passwörter nicht kennt.

Rufnummer (Ziel)

Für jedes Ziel muss eine Rufnummer definiert sein, da der Client sonst keine Verbindung herstellen kann. Diese Rufnummer muss genauso eingetragen werden, als würden Sie diese Telefonnummer per Hand wählen. D.h. Sie müssen alle notwendigen Vorwahlziffern berücksichtigen: Landesvorwahl, Ortsvorwahl, Durchwahlziffern, etc. etc.

Tragen Sie jedoch nicht die Amtsholung ein, auch wenn Sie an einer Nebenstellenanlage angeschlossen sind! Die Amtsholung wird unter dem Monitor-Menüpunkt “Konfiguration” eingetragen und hat auf diese Weise Gültigkeit für alle Rufe (→ siehe – Amtsholung).

Beispiel: Sie wollen eine Verbindung von Deutschland nach England herstellen
00 (für die internationale Verbindung, wenn Sie von Deutschland aus wählen)
44 (dies ist die landesspezifische Vorwahl für England)
171 (Vorwahl für London)
1234567 (die Nummer, die Sie zu erreichen wünschen)

Insgesamt wird nach diesem Beispiel folgende Nummer im Telefonbuch gespeichert und für die Anwahl verwendet: 00441711234567
Die Rufnummer des Ziels kann bis zu 30 Ziffern beinhalten.

Hinweis: Wenn ein Zielsystem eine Verbindung zu Ihrem PC über Rückruf aufbauen will, benötigt der Client diese Rufnummer in diesem Feld, um den Rückruf, entsprechend des gewählten Rückrufmodus annehmen zu können.

■ Alternative Rufnummern

Möglicherweise ist das Zielsystem ein Network Access Server (NAS), der mit mehreren S0-Anschlüssen für verschiedene Rufnummern ausgestattet ist. In diesen Fall empfiehlt es sich, alternative Rufnummern einzugeben – falls zum Beispiel die erste Nummer besetzt ist. Die alternativen Rufnummern werden der ersten Nummer angehängt, nur mit einem Doppelpunkt (:) oder einem Semikolon (;) getrennt.

Maximal werden 8 alternative Rufnummern unterstützt.

Beispiel : 000441711234567:000441711234568

Die erste Nummer ist die Standard-Rufnummer und wird immer zuerst gewählt. Kann keine Verbindung hergestellt werden, weil besetzt ist, wird die zweite Nummer gewählt, usw.

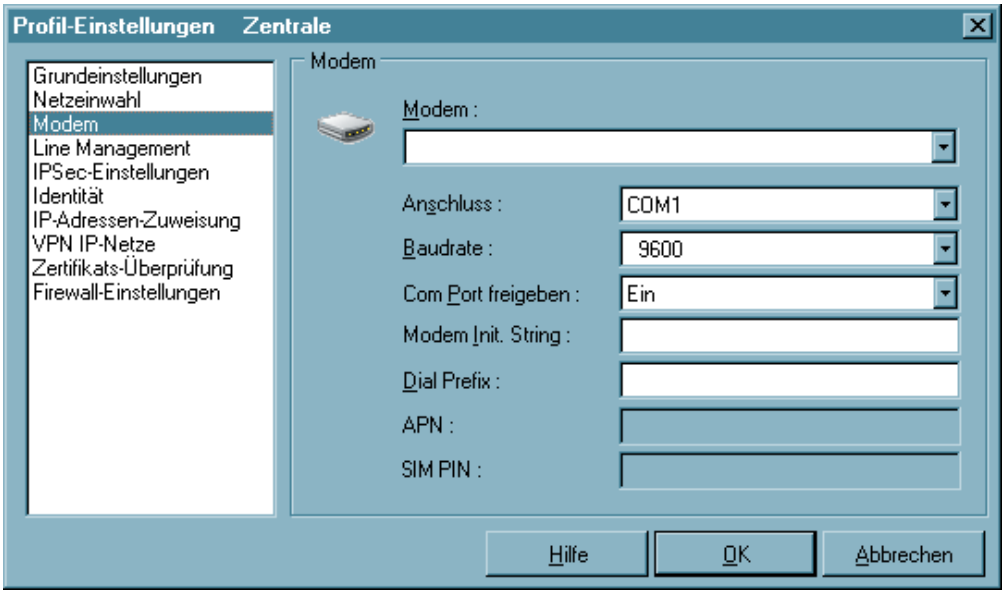
Wichtig: Bitte beachten Sie, dass der Verbindungsaufbau nur funktionieren kann, wenn die Protokoll-Eigenschaften für die Anschlüsse der alternativen Rufnummern die gleichen sind.

■ Script-Datei

Wenn Sie den Microsoft DFÜ-Dialer benutzen, tragen Sie hier die Script-Datei unter Eingabe von Pfad und Namen ein.

(Siehe → Grundeinstellungen, Micosoft DFÜ-Dialer verwenden)

4.1.3 Modem



Dieses Parameterfeld erscheint ausschließlich, wenn Sie als “Verbindungmedium” “Modem” gewählt haben. Alle nötigen Parameter zu dieser Verbindungsart sind hier gesammelt.

Parameter:

- ☐ Modem
- ☐ Anschluss
- ☐ Baudrate
- ☐ Com Port freigeben
- ☐ Modem Init. String
- ☐ Dial Prefix
- ☐ APN
- ☐ SIM PIN

Modem

Dieses Parameterfeld zeigt die auf dem PC installierten Modems. Wählen Sie aus der Liste das gewünschte Modem aus.

Je nachdem, welches Modem Sie wählen, werden die zugehörigen Parameter “Com Port” und “Modem Init. String” automatisch in die Konfigurationsfelder des Telefonbuchs aus der Treiberdatenbank des Systems übernommen.

(Weitere Parameter für dieses Kommunikationsmedium können auch über die Systemsteuerung des PCs konfiguriert werden.)

Hinweis: Bitte beachten Sie, dass Sie das Modem vor der Konfiguration der Verbindung im Telefonbuch installiert haben müssen, um es korrekt für Kommunikationsverbindungen nutzen zu können.

Anschluss

An dieser Stelle bestimmen Sie, welcher Com Port von Ihrem Modem genutzt werden soll. Wenn Sie bereits Modems unter Windows installiert haben, wird der während dieser Installation festgesetzte Com Port automatisch übernommen, sobald Sie das entsprechende Gerät unter “Modem” auswählen.

Hinweis: Wenn Sie ein bereits unter Ihrem System installiertes Modem nutzen möchten, so wählen Sie vor der Einstellung des Com Ports zuerst das gewünschte Gerät unter “Modem” aus – der entsprechend konfigurierte Com Port wird dann automatisch gesetzt.

Baudrate

Die Baudrate beschreibt die Übertragungsgeschwindigkeit zwischen Com Port und Modem. Wenn Ihr Modem z.b. mit 14.4 Kbits übertragen kann, sollten sie die nächsthöhere Baudrate 19200 wählen.

Folgende Baudraten können gewählt werden:
1200, 2400, 4800, 9600, 19200, 38400, 57600 und 115200

Com Port freigeben

Wenn Sie für Ihren Client ein analoges Modem verwenden, kann es wünschenswert sein, dass der Com Port nach Beendigung der Kommunikation für andere Applikationen freigegeben wird (z.B. Fax). In diesem Fall stellen Sie den Parameter auf “Ein”. Solange der Parameter in der Standardstellung auf ”Aus” bleibt, wird der Com Port ausschließlich von der Client Software genutzt.

Modem Init. String

Je nach eingesetzem Handy oder Modem und der jeweiligen Verbindungsart können AT-Kommandos nötig sein. In diesem Fall müssen die jeweiligen Kommandos dem zugehörigen Benutzerhandbuch oder den Mitteilungen der Telefongesellschaft bzw. des Providers entnommen werden. Jedes der in diesem Fall einzutragenden Kommandos muss mit einem <cr> (Carriage Return) abgeschlossen werden.

Dial Prefix

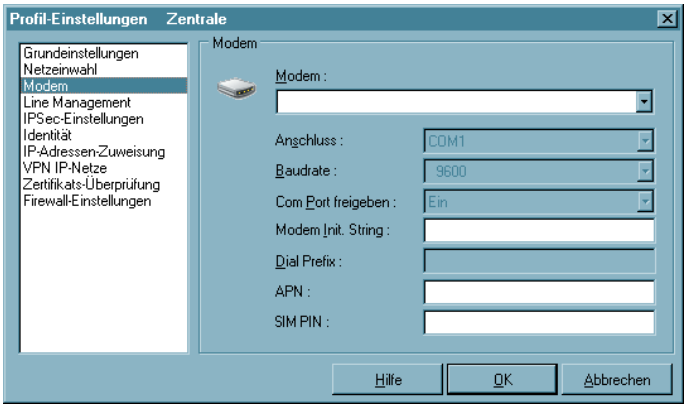
Dieses Feld ist optional. Ist das Modem korrekt installiert und steht der Software als Standardtreiber zur Verfügung, so muss hier kein Eintrag vorgenommen werden. Der Dial Prefix ist nur in seltenen Ausnahmefällen nötig. Ziehen Sie dazu das Modem-Handbuch zu Rate.

Im folgenden einige Beispiele für Dial Prefix:

ATDT
ATDP
ATDI
ATDX

APN

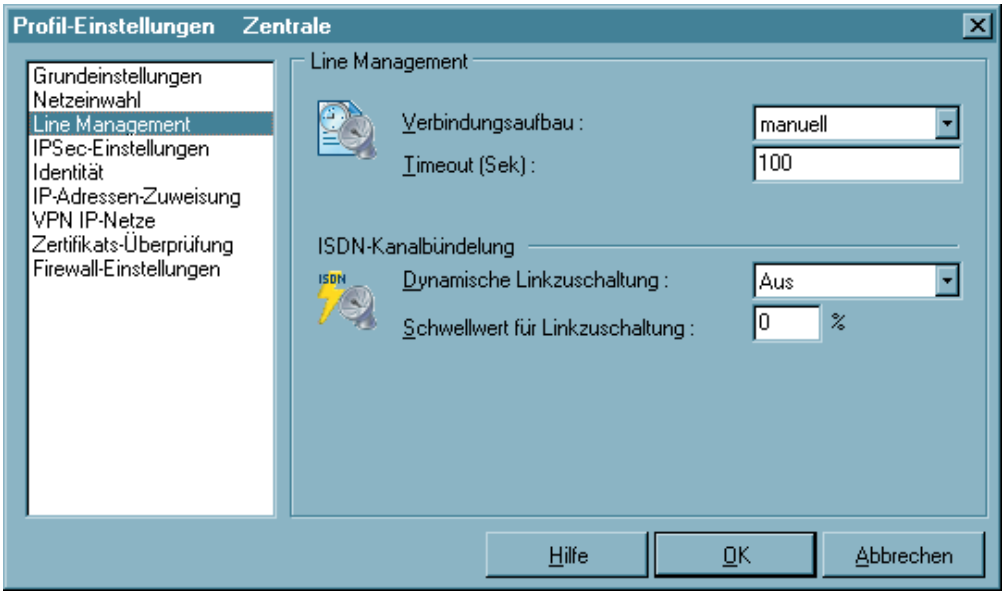
Der APN (Access Point Name) wird für die GPRS- und UMTS-Einwahl benötigt. Sie erhalten ihn von Ihrem Provider. Der APN wird insbesondere zu administrativen Zwecken genutzt.



SIM PIN

Benutzen Sie eine SIM-Einsteckkarte für GPRS oder UMTS, so geben Sie hier die PIN für diese Karte ein. Benutzen Sie ein Handy, so muss diese PIN am Mobiltelefon eingegeben werden.

4.1.4 Line Management



In diesem Parameterfeld bestimmen Sie, wie der “Verbindungsaufbau” erfolgen soll und stellen die Timeout-Werte ein.

Wenn der Client das Verbindungsmedium “ISDN” nutzt, können Sie in diesem Parameterfeld auch eine Kanalbündelung aktivieren. Bitte beachten Sie dabei, dass die Kanalbündelung nur funktionieren kann, wenn sowohl der Client als auch der NAS für eine Verbindung über gleich viele mögliche Kanäle verfügen.

Parameter:

- ☐ Verbindungsaufbau
- ☐ Timeout
- ☐ Dynamische Linkzuschaltung
- ☐ Schwellwert für Linkzuschaltung

■ Verbindungsaufbau

Hier definieren Sie, wie die Verbindung zu einem, im Telefonbuch eingetragenen Zielsystem, aufgebaut werden soll. Drei Modi stehen zur Wahl:

automatisch	=	(default) Dies bedeutet, dass die Client Software die Verbindung zum Zielsystem automatisch herstellt. Das Trennen der Verbindung erfolgt je nach Protokoll Ihres Systems, entsprechend den Anforderungen der Anwendung und den Einstellungen im Telefonbuch.
manuell	=	In diesem Fall müssen Sie die Verbindung zum Zielsystem manuell herstellen. Ein Trennen der Verbindung erfolgt je nach eingestelltem Wert für den Timeout.
wechselnd	=	Wird dieser Modus gewählt, muss zunächst die Verbindung “manuell” aufgebaut werden. Danach wechselt der Modus je nach Verbindungsabbau: – Wird die Verbindung nun mit Timeout beendet, so wird die Verbindung bei der nächsten Anforderung “automatisch” hergestellt, – wird die Verbindung manuell abgebaut, muss sie auch wieder manuell aufgebaut werden.

Wichtig: Sollten Sie den Verbindungsaufbau auf “manuell” setzen, so sollten Sie den Timeout aktivieren, um den Verbindungsabbau zu automatisieren. Andernfalls könnten unnötige Verbindungskosten für Sie entstehen.

■ Timeout

Mit diesem Parameter wird der Zeitraum festgelegt, der nach der letzten Datenbewegung (Empfang oder Versenden) verstreichen muss, bevor automatisch ein Verbindungsabbau erfolgt. Der Wert wird in Sekunden zwischen 0 und 65535 angegeben. Der Standardwert ist “100".

Wenn Ihr Anschluss (ISDN oder analog) einen Gebührenimpuls erhält, verwendet die Client Software das Impulsintervall, um den optimalen Zeitpunkt des Verbindungsabbaus bezüglich dem von Ihnen gesetzten Wert zu ermitteln. Der nach Gebührentakt optimierte Timeout läuft im Hintergrund und hilft die Verbindungskosten zu reduzieren.

Hinweis: Um den Timeout zu aktivieren, ist es nötig, einen Wert zwischen 1 und 65356 einzutragen. Mit dem Wert “0" wird der automatische Timeout (Verbindungsabbau) nicht ausgeführt. Der Wert ”0" bedeutet, dass das Trennen der Verbindung manuell durchgeführt werden muss. Ziehen Sie bei diesem Parameter bitte Ihren Internet Provider oder Ihren Systemadministrator zu Rate.

Wichtig: Der Timer für das gewählte Zeitintervall läuft erst dann an, wenn keine Datenbewegung oder Handshaking mehr auf der Leitung stattfindet.

Dynamische Linkzuschaltung (Nur für ISDN)

Mit dynamischer Linkzuschaltung (für ISDN) kann die Client Software bis zu 8 ISDN B-Kanäle bündeln. Um diese Funktion in vollem Umfang nutzen zu können, muss allerdings Ihr PC wie auch das Zielsystem mit der nötigen Anzahl von So-Schnittstellen (4) ausgestattet sein.

Die dynamische Linkzuschaltung funktioniert nur, wenn sie auch vom Network Access Server des Zielsystems unterstützt wird. Mit dynamischer Linkzuschaltung erhöhen sich zwar die Kosten für jeden zugeschalteten B-Kanal, gleichzeitig verringern sie sich jedoch in gleichem Maße, weil sich die Übertragungsdauer entsprechend verkürzt!

Mit diesem Parameter bestimmen Sie, wie die Linkzuschaltung erfolgen soll. Drei Möglichkeiten stehen zur Auswahl:

Aus	(standard)
Tx	Links werden zugeschaltet, entsprechend der Bitrate abgehender Daten
Rx	Links werden zugeschaltet, entsprechend der Bitrate eingehender Daten
TxRx	Links werden sowohl nach der Bitrate sowohl eingehender als auch abgehender Daten zugeschaltet

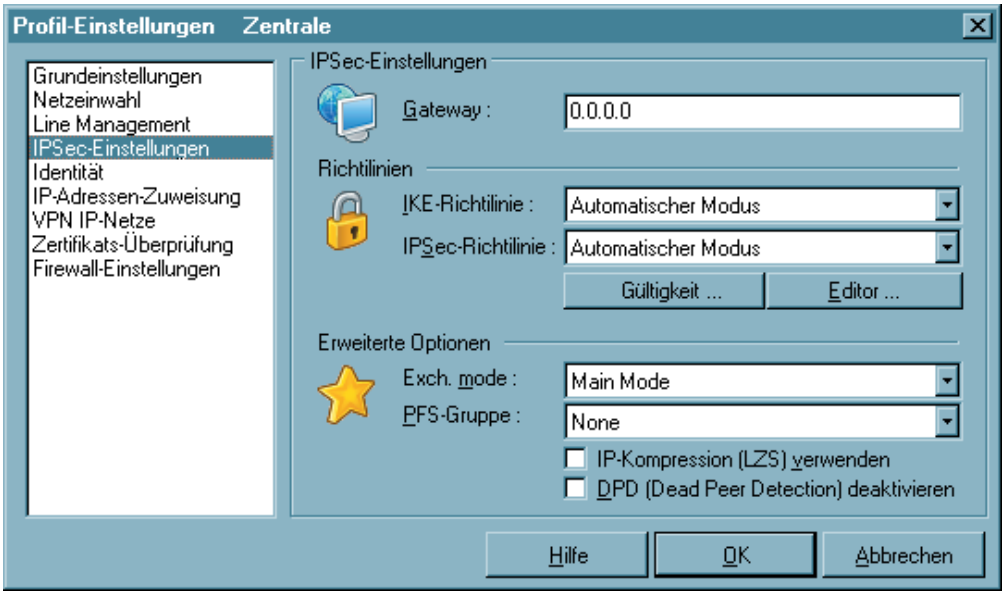
Schwellwert für Linkzuschaltung (Nur für ISDN)

Der Wert dieses Parameters teilt der Client Software die Bitrate mit, ab der ein weiterer Link (Kanal) zugeschaltet werden soll. Der Wert entspricht Prozenten der maximalen Bitrate. Mögliche Werte sind von 1 bis 100 (Prozent). Standardwert ist “20". Diese Einstellung gilt für Sender und Empfänger.

Die Zuschaltung eines weiteren Links erfolgt 8 Sekunden nach dem Erreichen des eingestellten Schwellwerts.

Diese Einstellung kommt nur zum Tragen, wenn die Linkzuschaltung aktiviert wurde.

4.1.5 IPSec-Einstellungen



In diesem Parameterfeld geben Sie die IP-Adresse des Gateways ein. Darüber hinaus legen Sie die Richtlinien fest, die für die IPSec-Verbindung in der Phase 1- und Phase 2-Verhandlung verwendet werden sollen. Sofern der automatische Modus genutzt wird, akzeptiert der Client die Richtlinien, wie sie vom Gateway der Gegenstelle vorgegeben werden. Soll der IPSec Client als Initiator der Verbindung eigene Richtlinien verwenden, so müssen diese mit dem Richtlinien-Editor konfiguriert werden. Die erweiterten Optionen können nach Abstimmung mit der Gegenstelle eingesetzt werden.

Parameter:

- ☐ Gateway
- ☐ IKE-Richtlinie
- ☐ IPSec-Richtlinie
- ☐ Richtlinien-Gültigkeit
- ☐ Richtlinien-Editor
- ☐ Exch. Mode
- ☐ PFS-Gruppe
- ☐ IP-Kompression (LZS) verwenden
- ☐ DPD (Dead Peer Detection) deaktivieren

Gateway

Dies ist die IP-Adresse des IPSec Gateways, auch Tunnel-Endpunkt. Sie erhalten die Adresse von Ihrem Administrator entweder als Hex-Adresse, wenn das Gateway über eine feste offizielle IP-Adresse verfügt – oder als Namens-String, wenn das Gateway eine wechselnde IP-Adresse von einem Internet Service Provider erhält.

Hex-Adresse: Die Adresse ist 32 Bits lang und besteht aus vier voneinander durch Punkte getrennte Zahlen.

Namens-String: Sie tragen den Namen ein, den Sie von Ihrem Administrator erhalten haben. Es handelt sich dabei um den DNS-Namen des Gateways, der beim DynDNS Service Provider hinterlegt wurde.

IKE-Richtlinie

Die IKE-Richtlinie wird aus der Listbox ausgewählt. In der Listbox werden alle IKE-Richtlinien aufgeführt, die Sie im Richtlinien-Editor unter der Verzweigung “IKE-Richtlinie” angelegt haben. Die Richtlinien erscheinen in der Box mit dem Namen, den Sie bei der Konfiguration vergeben haben.

Sie finden zwei vorkonfigurierte Richtlinien im Richtlinien-Editor unter “IKE-Richtlinie” als “Pre-shared Key” und “RSA-Signatur”. Inhalt und Name dieser Richtlinien können jederzeit geändert werden, bzw. neue Richtlinien können hinzugefügt werden. Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu Authentisierung und Verschlüsselungsalgorithmus auf (siehe → IKE-Richtlinie (editieren)), d.h. eine Richtlinie besteht aus verschiedenen Vorschlägen. Funktional unterscheiden sich diese Richtlinien durch Verwendung eines statischen Schlüssels bzw. einer RSA-Signatur.

Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D.h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Automatischer Modus: In diesem Fall kann die Konfiguration der IKE-Richtlinie mit dem im Richtlinien-Editor entfallen. Die Richtlinie wird vom Gateway der Gegenstelle vorgegeben und vom Client akzeptiert.

Pre-shared Key: Diese vorkonfigurierte Richtlinie kann ohne PKI-Unterstützung genutzt werden. Beidseitig wird der gleiche “Statische Schlüssel” verwendet (siehe → Pre-shared Key verwenden, Shared Secret im Parameterfeld “Identität”).

RSA-Signatur: Diese vorkonfigurierte Richtlinie kann nur mit PKI-Unterstützung eingesetzt werden. Als zusätzliche, verstärkte Authentisierung ist der Einsatz der RSA-Signatur nur sinnvoll unter Verwendung einer Smart Card oder eines Soft-Zertifikats.

■ IPSec-Richtlinie

Die IPSec-Richtlinie wird aus der Listbox ausgewählt. In der Listbox werden alle IP-Sec-Richtlinien aufgeführt, die Sie mit dem Richtlinien-Editor angelegt haben. Die Richtlinien erscheinen in der Box mit dem Namen, den sie bei der Konfiguration vergeben haben.

Funktional unterscheiden sich zwei IPSec-Richtlinien nach dem IPSec-Sicherheitsprotokoll AH (Authentication Header) oder ESP (Encapsulating Security Payload). Da der IPSec-Modus mit AH-Sicherung für flexiblen Remote Access völlig ungeeignet ist, wird nur die IPSec-Richtlinie mit ESP-Protokoll, “ESP - 3DES - MD5", standardmäßig vorkonfiguriert mit der Software ausgeliefert.

Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu IPSec-Protokoll und Authentisierung auf (siehe → IPSec-Richtlinie (editieren)), d.h. eine Richtlinie besteht aus verschiedenen Vorschlägen.

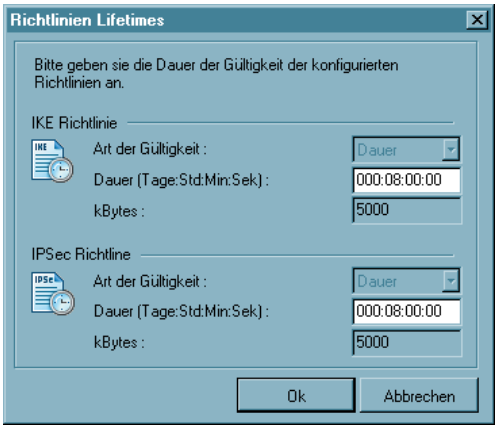
Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D.h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Automatischer Modus: In diesem Fall kann die Konfiguration der IKE-Richtlinie mit dem Richtlinien-Editor entfallen.

ESP - 3DES - MD5 (oder anderer Richtlinien-Name): Wenn Sie den Namen der vorkonfigurierten IPSec-Richtlinie wählen, muss die gleiche Richtlinie mit all ihren Vorschlägen für alle Benutzer gültig sein. Dies bedeutet, dass sowohl auf Client- als auch auf Server-Seite die gleichen Vorschläge für die Richtlinien zur Verfügung stehen müssen.

Richtlinien-Gültigkeit

Die hier definierte Dauer der Gültigkeit gilt für alle Richtlinien gleichermaßen.

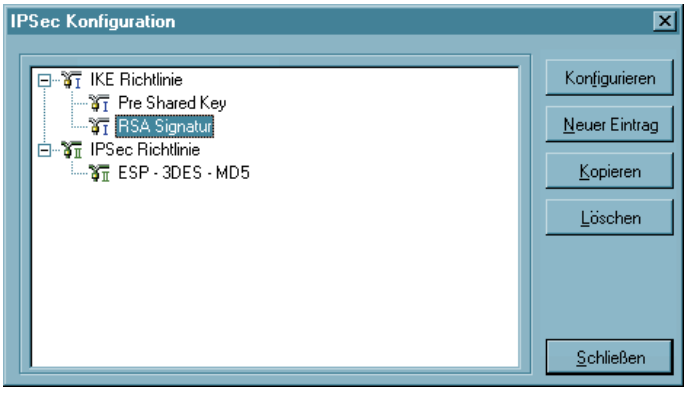


■ Dauer

Die Menge der kBytes oder die Größe der Zeitspanne kann eigens eingestellt werden.

Richtlinien-Editor

Zur Konfiguration der Richtlinien und gegebenenfalls einer statischen Secure Policy Database wird dieser Menüpunkt angeklickt. Damit öffnet sich ein Konfigurationsfenster mit der Verzweigung der Richtlinien und Secure Policy Database zu IPSec, sowie Buttons zur Bedienung auf der rechten Seite des Konfigurationsfensters.



Um die (Standard-)Werte der Richtlinien zu editieren, wählen Sie mit der Maus die Richtlinie, deren Werte Sie ändern möchten – die Buttons zur Bedienung werden dann aktiv.

Konfigurieren
Um eine Richtlinie oder eine SPD abzuändern, wählen Sie mit der Maus den Namen, der Gruppe deren Werte Sie ändern möchten und klicken auf “Konfigurieren”. Dann öffnet sich das entsprechende Parameterfeld mit den IPSec-Parametern.

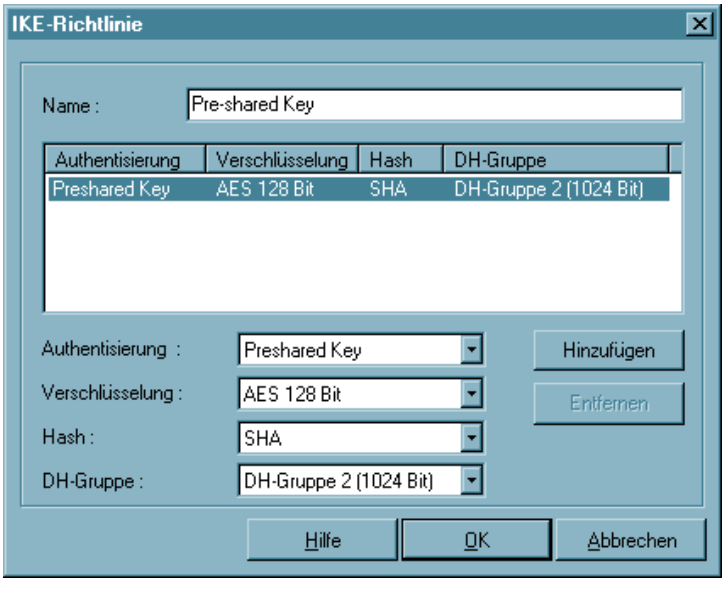
Neuer Eintrag
Wenn Sie eine neue Richtlinie oder SPD anlegen möchten, selektieren Sie eine der Richtlinien oder die SPD und klicken auf “Neuer Eintrag”. Die neue Richtlinie oder SPD wird erzeugt. Alle Parameter sind auf Standardwerte gesetzt, bis auf den Namen.

Kopieren
Um die Parameter-Einstellungen eines bereits definierten Richtlinie oder SPD zu kopieren, markieren sie die zu kopierende Richtlinie oder SPD und klicken auf “Kopieren”. Daraufhin wird das Parameterfeld geöffnet. Ändern Sie nun den Namen und klikken Sie anschließend Ok. Die neue Richtlinie oder SPD ist nun angelegt. Die Parameterwerte sind zu denen der kopierten identisch, bis auf den Namen.

Löschen
Wenn Sie eine Richtlinie oder SPD aus dem Konfigurationsbaum löschen wollen, selektieren Sie sie und klicken auf “Löschen”. Die Richtlinie oder SPD ist damit auf Dauer aus der IPSec-Konfiguration gelöscht.

Schließen
Wenn Sie das IPSec-Feld schließen, kehren Sie zum Monitor zurück. Die Daten werden so wie sie konfiguriert wurden behalten.

IKE-Richtlinie (editieren)



Die Parameter in diesem Feld beziehen sich auf die Phase 1 des Internet Key Exchange (IKE) mit dem der Kontrollkanal für die SA-Verhandlung aufgebaut wird. Den IKE-Modus (Austausch-Modus / Exchange Mode), Main Mode oder Aggressive Mode, bestimmen Sie in dem Parameterfeld “IPSec-Einstellungen” im Telefonbuch. Die IKE-Richtlinien, die Sie hier konfigurieren, werden zur Auswahl gelistet.

Inhalt und Name dieser Richtlinien können jederzeit geändert werden, bzw. neue Richtlinien können hinzugefügt werden. Jede Richtlinie listet mindestens einen Vorschlag (Proposal) zu Authentisierung und Verschlüsselungsalgorithmus auf, d.h. eine Richtlinie kann aus mehreren Vorschlägen bestehen.

Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D.h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Mit den Buttons “Hinzufügen” und “Entfernen” erweitern Sie die Liste der Vorschläge oder löschen einen Vorschlag aus der Liste der Richtlinie.

Parameter:

- ☐ Name | IKE-Richtlinie
- ☐ Authentisierung | IKE-Richtlinie
- ☐ Verschlüsselung | IKE-Richtlinie
- ☐ Hash | IKE-Richtlinie
- ☐ DH-Gruppe | IKE-Richtlinie

Name | IKE-Richtlinie

Geben Sie dieser Richtlinie einen Namen, über den sie später einer SPD zugeordnet werden kann.

Authentisierung | IKE-Richtlinie

Bevor der Kontrollkanal für die Phase 1-Verhandlung (IKE Security Association) aufgebaut werden kann, muss beidseitig eine Authentisierung stattgefunden haben.

Zur gegenseitigen Authentisierung wird der allen gemeinsame pre-shared Key (statischer Schlüssel) verwendet. Diesen Schlüssel definieren Sie im Parameterfeld “Identität”.

Verschlüsselung | IKE-Richtlinie

Nach einem der optionalen Verschlüsselungsalgorithmen erfolgt die symmetrische Verschlüsselung der Messages 5 und 6 im Kontrollkanal, sofern der Main Mode (Identity Protection Mode) gefahren wird. Zur Wahl stehen: DES, Triple DES, Blowfish, AES 128, AES 192, AES 256.

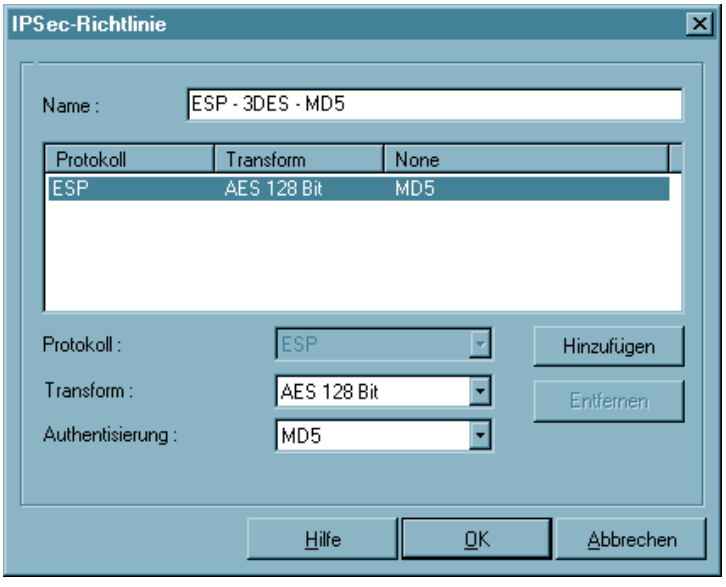
Hash | IKE-Richtlinie

Modus, wie der Hash-Wert über die ID bzw. das Zertifikat der Messages im Kontrollkanal gebildet wird. Zur Wahl stehen: MD5 (Message Digest, Version 5) und SHA (Secure Hash Alogrithm).

DH-Gruppe | IKE-Richtlinie

Mit der Wahl einer der angebotenen Diffie-Hellman-Gruppen wird festgelegt, wie sicher der Key Exchange im Kontrollkanal erfolgen soll, nach dem der spätere symmetrische Schlüssel erzeugt wird. Je höher die DH Group desto sicherer ist der Key Exchange.

IPSec-Richtlinie (editieren)



Die IPSec-Richtlinien (Phase-2-Parameter), die Sie hier konfigurieren, werden zur Auswahl für die SPD gelistet.

Für alle Benutzer sollten die gleichen Richtlinien samt zugehöriger Vorschläge (Proposals) gelten. D.h. sowohl auf Client-Seite als auch am Zentralsystem sollten für die Richtlinien (Policies) die gleichen Vorschläge (Proposals) zur Verfügung stehen.

Mit den Buttons “Hinzufügen” und “Entfernen” erweitern Sie die Liste der Vorschläge oder löschen einen Vorschlag aus der Liste der Richtlinie.

Parameter:

- ☐ Name | IPSec-Richtlinie
- ☐ Protokoll | IPSec-Richtlinie
- ☐ Transformation | IPSec-Richtlinie
- ☐ Authentisierung | IPSec-Richtlinie

Name | IPSec-Richtlinie

Geben Sie dieser Richtlinie einen Namen, über den Sie sie später einer SPD zuordnen können.

Protokoll | IPSec-Richtlinie

Der fest eingestellte Standardwert ist ESP.

Transformation | IPSec-Richtlinie

Wenn das Sicherheitsprotokoll ESP eingestellt wurde, kann hier definiert werden wie mit ESP verschlüsselt werden soll. Zur Wahl stehen die gleichen Verschlüsselungsalgorithmen wie für Layer 2:

DES, Triple DES, Blowfish, AES 128, AES 192, AES 256.

Authentisierung | IPSec-Richtlinie

Für das Sicherheitsprotokoll ESP kann der Modus der Authentisierung eigens eingestellt werden. Zur Wahl stehen: MD5 und SHA.

Erweiterte Optionen

Exch. Mode

Der Exchange Mode (Austausch-Modus) bestimmt wie der Internet Key Exchange vonstatten gehen soll. Zwei unterschiedliche Modi stehen zur Verfügung, der Main Mode, auch Identity Protection Mode und der Aggressive Mode. Die Modi unterscheiden sich durch die Anzahl der Messages und durch deren Verschlüsselung.

Main Mode: Im Main Mode (Standard-Einstellung) werden sechs Meldungen über den Kontrollkanal geschickt, wobei die beiden letzten, welche die User ID, das Zertifikat die Signatur und ggf. einen Hash-Wert beinhalten, verschlüsselt werden – daher auch Identity Protection Mode.

Aggressive Mode: Im Aggressive Mode gehen nur drei Meldungen über den Kontrollkanal, wobei nichts verschlüsselt wird.

PFS-Gruppe

Mit Auswahl einer der angebotenen Diffie-Hellman-Gruppen wird festgelegt, ob ein kompletter Diffie-Hellman-Schlüsselaustausch (PFS, Perfect Forward Secrecy) in Phase 2 zusätzlich zur SA-Verhandlung stattfinden soll. Standard ist “keine”.

IP-Kompression (LZS) verwenden

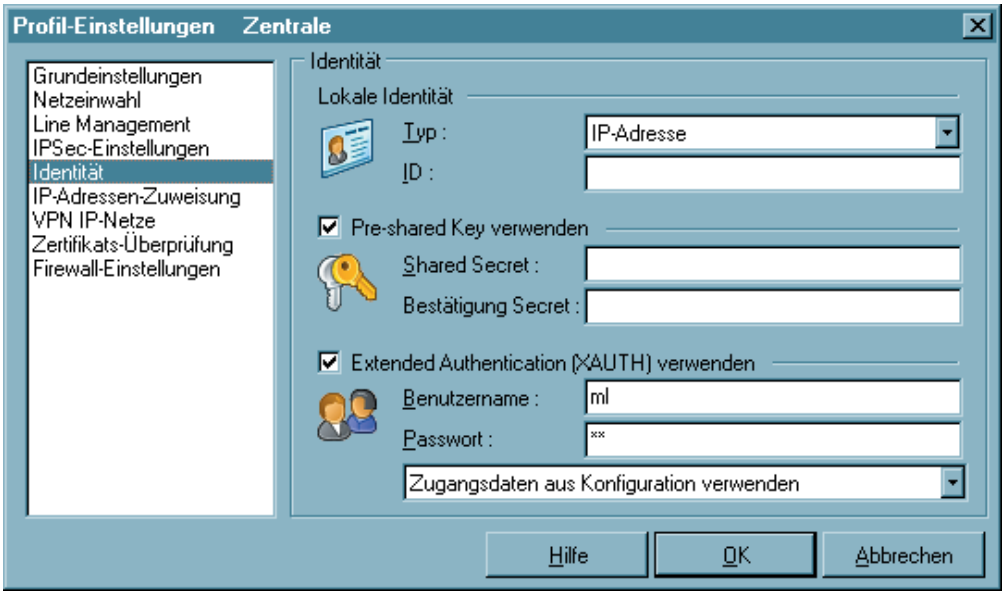
Die Datenübertragung mit IPSec kann ebenso komprimiert werden wie ein Transfer ohne IPSec. Dies ermöglicht eine Steigerung des Durchsatzes um maximal das 3-fache.

DPD (Dead Peer Detection) deaktivieren

DPD (Dead Peer Detection) und NAT-T (NAT Traversal) werden automatisch im Hintergrund ausgeführt, sofern dies das Ziel-Gateway unterstützt. Der IPSec Client nutzt DPD, um in regelmäßigen Intervallen zu prüfen, ob die Gegenstelle noch aktive ist. Ist dies nicht der Fall erfolgt ein automatischer Verbindungsabbau.

Mit dieser Funktion kann DPD ausgeschaltet werden.

4.1.6 Identität



Entsprechend des Sicherheitsmodus IPSec können noch detailliertere Sicherheitseinstellungen vorgenommen werden.

Parameter:

☐ Typ | Identität

☐ ID | Identität

☐ Pre-shared Key verwenden

☐ Extended Authentication (XAUTH) verwenden

☐ Benutzername | Identität

☐ Passwort | Identität

☐ Zugangsdaten aus Konfiguration verwenden

Typ | Identität

Bei IPSec wird zwischen abgehenden und eingehenden Verbindungen unterschieden. Der Wert, den der Initiator als ID für eine abgehende Verbindung gewählt hat, muss bei der Gegenstelle als ID für eingehende Verbindungen gewählt sein.

Folgende ID-Typen stehen zur Auswahl:
– IP Address
– Fully Qualified Domain Name
– Fully Qualified Username
(entspricht der E-Mail-Adresse des Benutzers)
– IP Subnet Address
– ASN1 Distinguished Name
– ASN1 Group Name
– Free String used to identify Groups

ID | Identität

Bei IPSec wird zwischen abgehenden und eingehenden Verbindungen unterschieden. Der Wert, den der Initiator als ID für eine abgehende Verbindung gewählt hat, muss bei der Gegenstelle als ID für eingehende Verbindungen gewählt sein.

Entsprechend dem ID-Typ muss die zugehörige ID als String eingetragen werden.

Pre-shared Key verwenden

Der Pre-shared Key ist ein String beliebiger Zeichen in einer maximalen Länge von 255 Zeichen. Alle alphanumerischen Zeichen können verwendet werden. Wenn die Gegenstelle einen pre-shared Key während der IKE-Verhandlung erwartet, dann muss dieser Schlüssel in das Feld “Shared Secret” eingetragen werden.

Bestätigen Sie das “Shared Secret” im darunter liegenden Feld. Der gleiche pre-shared Key muss auf beiden Seiten verwendet werden.

Extended Authentication (XAUTH) verwenden

Wird “IPSec-Tunneling” genutzt, so kann die Authentisierung über Extended Authentication (XAUTH Protokoll, Draft 6) erfolgen. Wird XAUTH eingesetzt und vom Gateway untersützt, so aktivieren Sie “Benutze erweiterte Authentisierung (XAUTH)”. Zusätzlich zum pre-shared Key können dann noch folgende Parameter gesetzt werden:

Benutzername = Benutzername des IPSec-Benutzers

Passwort = Kennwort des IPSec-Benutzers

Benutzername | Identität

Den Benutzernamen für XAUTH erhalten Sie von Ihrem Systemadministrator. Der Name kann 256 Zeichen lang sein.

Hinweis: Dieser Parameter wird nur benötigt, um Zugriff auf das Gateway der remote Seite zu bekommen.

Passwort | Identität

Das Passwort für XAUTH erhalten Sie von Ihrem Systemadministrator. Der Name kann 256 Zeichen lang sein.

Hinweis: Dieser Parameter wird nur benötigt, um Zugriff auf das Gateway der remote Seite zu bekommen.

Zugangsdaten aus Konfiguration verwenden

Als Zugangsdaten für das VPN können folgende Einträge ausgelesen und verwendet werden:

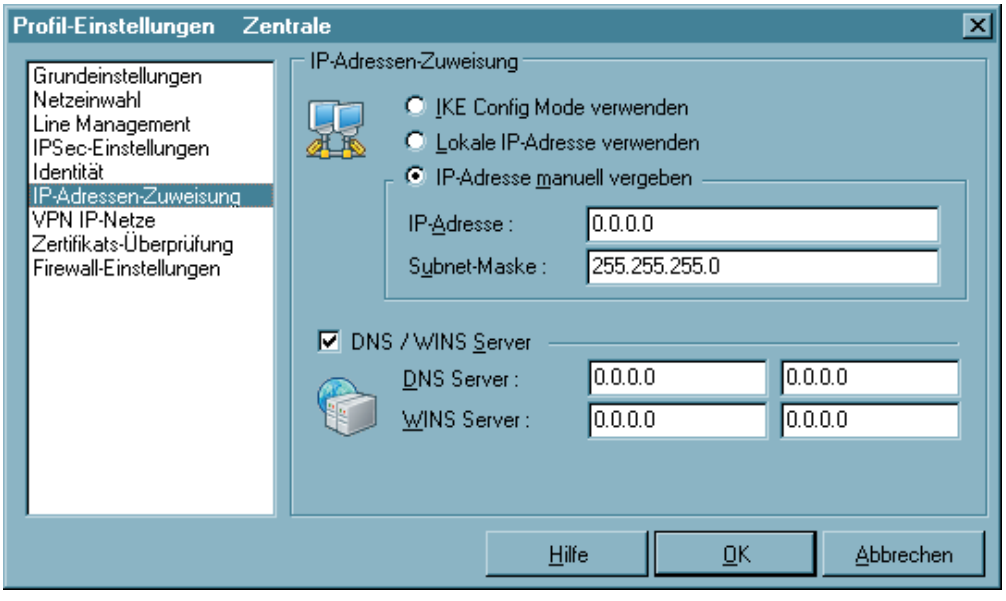
Zugangsdaten aus Konfiguration verwenden:
Dies bedeutet, dass die in diesem Parameterfeld unter “Benutzername” und “Passwort” gemachten Angaben zur erweiterten Authentisierung verwendet werden.

Zugangsdaten aus Zertifikat (E-Mail) verwenden:
Dies bedeutet, dass statt “Benutzername” und “Passwort” der E-Mail-Eintrag des Zertifikats verwendet wird.

Zugangsdaten aus Zertifikat (Common Name) verwenden:
Dies bedeutet, dass statt “Benutzername” und “Passwort” der Benutzer-Eintrag des Zertifikats verwendet wird.

Zugangsdaten aus Zertifikat (Seriennummer) verwenden:
Dies bedeutet, dass statt “Benutzername” und “Passwort” die Seriennummer des Zertifikats verwendet wird.

4.1.7 IP-Adressen-Zuweisung



Parameter:

- ☐ IKE Config Mode verwenden
- ☐ Lokale IP-Adresse verwenden
- ☐ IP-Adresse manuell vergeben
- ☐ DNS/WINS
- ☐ DNS-Server
- ☐ WINS-Server

IKE Config Mode verwenden

IP-Adressen und DNS Server werden über das Protokoll IKE-Config Mode (Draft 2) zugewiesen. Für die NAS-Einwahl können alle bisherigen WAN-Schnittstellen verwendet werden.

Bei “IPSec-Tunneling” wird im Hintergrund automatisch DPD (Dead Peer Detection) und NAT-T (NAT Traversal) ausgeführt, falls dies von der Gegenstelle unterstützt wird. Mit DPD prüft der Client in bestimmten Abständen, ob die Gegenstelle noch aktiv ist. Bei inaktiver Gegenstelle erfolgt ein automatischer Verbindungsabbau. Der Einsatz von NAT Traversal erfolgt beim Client automatisch und ist immer nötig, wenn auf Seiten des Zielsystems ein Gerät mit Network Address Translation zum Einsatz kommt.

Lokale IP-Adresse verwenden

In diesem Fall wird die aktuell in den Netzwerkeinstellungen des PCs konfigurierte IP-Adresse (auch DHCP) für den IPSec Client genutzt.

IP-Adresse manuell vergeben

Dies ist die IP-Adresse und die Subnet-Maske, die hier frei eingegeben werden können. In diesem Fall wird die hier eingetragene Adresse genutzt, unabhängig von der Konfiguration in den Netzwerkeinstellungen.

DNS/WINS

Mit IKE Config Mode werden dynamisch IP-Adressen des Clients, des DNS- und WINS-Servers sowie der Domain Name zugewiesen.

Wird diese Funktion aktiviert, so kann alternativ zu dem DNS/WINS-Server, der automatisch während der PPP-Verhandlung zum NAS/ISP zugewiesen wird, ein anderer DNS/WINS Server bestimmt werden.

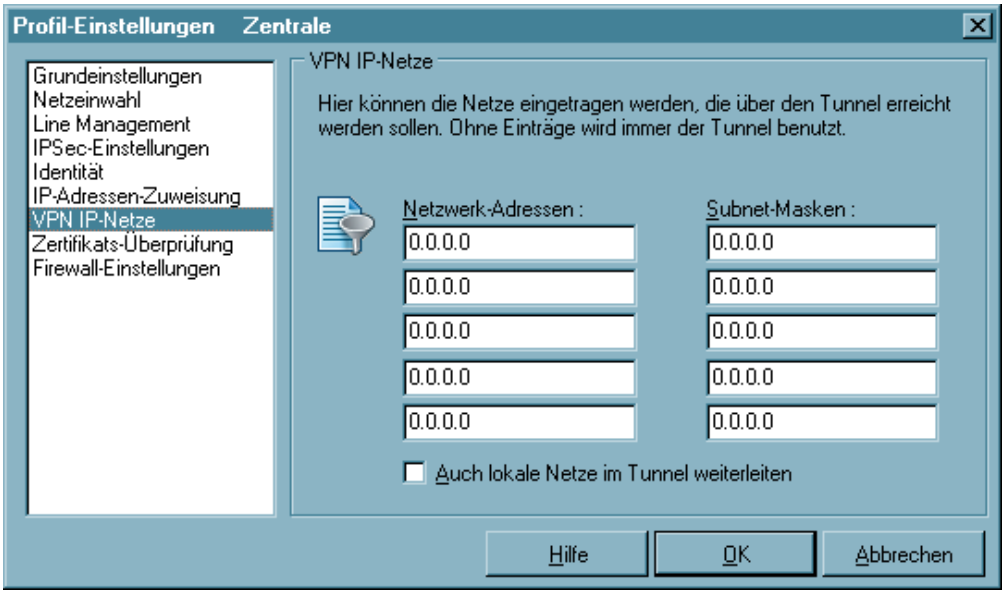
DNS-Server

Der zuerst eingetragene DNS-Server wird anstatt des über PPP-Verhandlung ermittelten Servers genutzt.

WINS-Server

Der zuerst eingetragene WINS-Server wird anstatt des über PPP-Verhandlung ermittelten Servers genutzt.

4.1.8 VPN IP-Netze



Hier können genau die IP-Netze definiert werden, über die der Client via VPN-Tunnel komunizieren kann. Wenn Tunneling genutzt wird und hier keine Einträge erfolgen, so wird die Verbindung immer zum Tunnel-Endpunkt des Gateways aufgebaut. Soll alternierend einerseits ein Tunneling zur Zentrale erfolgen, andererseits über das Internet kommuniziert werden, so müssen hier die IP-Netze eingetragen werden, die vom Client erreicht werden sollen. Sie können dann zwischen dem Internet und dem Gateway der Firmenzentrale hin und her springen. Dies wird auch als “Split Tunneling” bezeichnet.

Parameter:

- ☐ Netzwerk-Adressen | VPN IP-Netze
- ☐ Subnet-Masken
- ☐ Auch lokale Netze im Tunnel weiterleiten

Netzwerk-Adressen | VPN IP-Netze

In diesem Parameterfenster definieren Sie, in welchem IP-Netz oder welchen IP-Netzen der Client über VPN-Tunneling kommunizieren kann. Sie erhalten die Adresse(n) von Ihrem Systemadministrator.

Bitte achten Sie ferner darauf, daß die IP-Adresse des Gateways nicht im Bereich der Netz-Adresse liegt.

Subnet-Masken

Hier tragen Sie die zugehörige Netzmaske des IP-Netzes ein. Sie erhalten die Adresse(n) von Ihrem Systemadministrator.

Bitte achten Sie darauf, daß die IP-Adresse des Gateways nicht im Bereich der Netz-Adresse liegt.

Auch lokale Netze im Tunnel weiterleiten

Wenn der Datenverkehr des lokalen Netzes über VPN-Tunneling weitergeleitet werden soll, so muss diese Funktion aktiviert werden.

4.1.9 Zertifikats-Überprüfung

Im Parameterfeld “Zertifikats-Überprüfung” kann pro Zielsystem des IPSec Clients vorgegeben werden, welche Einträge in einem Zertifikat der Gegenstelle (Gateway) vorhanden sein müssen (siehe → Eingehendes Zertifikat anzeigen, Allgemein).

Siehe auch:

- ☐ Benutzer des eingehenden Zertifikats
- ☐ Aussteller des eingehenden Zertifikats
- ☐ Fingerprint des Aussteller-Zertifikats
- ☐ SHA1 Fingerprint verwenden
- ☐ Weitere Zertifikats-Überprüfungen

Benutzer des eingehenden Zertifikats

Als Einträge des Benutzer-Zertifikats der Gegenstelle (Server) können alle Attribute des Benutzers, soweit bekannt – auch mit Wildcards -, verwendet werden. Vergleichen Sie dazu, welche Einträge bei “eingehendes Zertifikat anzeigen” unter Benutzer aufgeführt sind.

Verwenden Sie die Kürzel der Attributtypen. Die Kürzel der Attributtypen für Zertifikatseinträge haben folgende Bedeutung:

```
cn     = Common Name / Name
s      = Surname / Nachname
g      = Givenname / Vorname
t      = Title / Titel
o      = Organisation / Firma
ou     = Organization Unit / Abteilung
c      = Country / Land
st     = State / Bundesland, Provinz
l      = Location / Stadt, Ort
email  = E-mail
```

Beispiel:
`cn=VPNGW*, o=ABC, c=de`
Der Common Name des Security Servers wird hier nur bis zur Wildcard “*” überprüft. Alle nachfolgenden Stellen können beliebig sein, etwa 1 - 5 als Numerierung. Die Organzation Unit muss in diesem Fall immer ABC sein und das Land Deutschland.

Aussteller des eingehenden Zertifikats

Als Einträge des Benutzer-Zertifikats der Gegenstelle (Server) können alle Attribute des Ausstellers, soweit bekannt – auch mit Wildcards -, verwendet werden. Vergleichen Sie dazu welche Einträge bei “eingehendes Zertifikat anzeigen” unter Aussteller aufgeführt sind.

Verwenden Sie die Kürzel der Attributtypen. Die Kürzel der Attributtypen für Zertifikatseinträge haben folgende Bedeutung:

```
cn     = Common Name / Name
s      = Surname / Nachname
g      = Givenname / Vorname
t      = Title / Titel
o      = Organisation / Firma
ou     = Organization Unit / Abteilung
c      = Country / Land
st     = State / Bundesland, Provinz
l      = Location / Stadt, Ort
email  = E-mail
```

Beispiel:
`cn=ABC GmbH`
Hier wird nur der Common Name des Ausstellers überprüft.

■ Fingerprint des Aussteller-Zertifikats

Um zu verhindern, dass ein Unberechtigter, der die vertrauenswürdige CA imitiert, ein gefälschtes Aussteller-Zertifikat verwenden kann, kann zusätzlich der Fingerprint des Ausstellers, soweit bekannt, eingegeben werden.

■ SHA1 Fingerprint verwenden

Der Algorithmus zur Erzeugung des Fingerprints kann MD5 (Message Digit 5) oder SHA1 (Secure Hash Algorithm 1) sein.

Weitere Zertifikats-Überprüfungen

Neben der Zertifikats-Überprüfung nach Inhalten erfolgt am IPSec Client eine weitere Zertifikatsprüfung in mehrfacher Hinsicht.

1. Auswahl der CA-Zertifikate

Der Administrator des Firmennetzes legt fest, welchen Ausstellern von Zertifikaten vertraut werden kann. Dies geschieht dadurch, dass er die CA-Zertifikate seiner Wahl in das Windows-Verzeichnis \ncple\cacerts\ gespielt. Das Einspielen kann bei einer Software-Distribution mit Disketten automatisiert stattfinden, wenn sich die Aussteller-Zertifikate bei der Installation der Software im Root-Verzeichnis der ersten Diskette befinden. Nachträglich können Aussteller-Zertifikate automatisch über den Secure Update Server verteilt werden (siehe → Handbuch zum Update Server), oder – sofern der Benutzer über die notwendigen Schreibrechte in genanntem Verzeichnis verfügt – von diesem selbst eingestellt werden (siehe → CA-Zertifikate anzeigen).

Derzeit werden die Formate *.pem und *.crt für Aussteller-Zertifikate unterstützt. Sie können im Monitor unter dem Hauptmenüpunkt “Verbindung, Zertifikate, CA-Zertifikate anzeigen” eingesehen werden.

Wird am IPSec Client das Zertifikat einer Gegenstelle empfangen, so ermittelt der Client den Aussteller und sucht anschließend das Aussteller-Zertifikat, zunächst auf Smart Card oder PKCS#12-Datei, anschließend im Verzeichnis NCPLE\CACERTS\. Kann das Aussteller-Zertifikat nicht gefunden werden, kommt die Verbindung nicht zustande.

Sind keine Aussteller-Zertifikate vorhanden, wird keine Verbindung zugelassen.

2. Überprüfung der Zertifikats-Erweiterung

Zertifikate können Erweiterungen (Extensions) erfahren. Diese dienen zur Verknüpfung von zusätzlichen Attributen mit Benutzern oder öffentlichen Schlüsseln, die für die Verwaltung und den Betrieb der Zerifizierungshierarchie und der Sperrlisten (Revocation Lists) benötigt werden. Prinzipiell können Zertifikate eine beliebige Anzahl von Erweiterungen inklusive privat definierter beinhalten. Die Zertifikats-Erweiterungen (Extensions) werden von der ausstellenden Certification Authority in das Zertifikat geschrieben.

Für den IPSec Client und das Gateway sind drei Erweiterungen von Bedeutung:
– extendedKeyUsage
– subjectKeyIdentifier
– authorityKeyIdentifier

extendedKeyUsage:

Befindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung extendedKeyUsage so prüft der IPSec Client, ob der definierte erweiterte Verwendungszweck “SSL-Server-Authentisierung” enthalten ist. Ist das eingehende Zertifikat nicht zur Server-Authentisierung vorgesehen, so wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

Bitte beachten Sie, dass die SSL-Server-Authentisierung richtungsabhängig ist. D.h. der Initiator des Tunnelaufbaus prüft das eingehende Zertifikat der Gegenstelle, das, sofern die Erweiterung extendedKeyUsage vorhanden ist, den Verwendungszweck “SSL-Server-Authentisierung” beinhalten muss. Dies gilt auch bei einem Rückruf an den Client über VPN.

subjectKeyIdentifier / authorityKeyIdentifier:

Ein keyIdentifier ist eine zusätzliche ID (Hashwert) zum CA-Namen auf einem Zertifikat. Der authorityKeyIdentifier (SHA1-Hash über den public Key des Ausstellers) am eingehenden Zertifikat muss mit dem subjectKeyIdentifier (SHA1-Hash über den public Key des Inhabers) am entsprechenden CA-Zertifikat übereinstimmen. Kann keine Übereinstimmung erkannt werden, wird die Verbindung abgelehnt.

Der keyIdentifier kennzeichnet den öffentlichen Schlüssel der Zertifizierungsstelle und somit nicht nur eine, sondern gegebenenfalls eine Reihe von Zertifikaten. Damit erlaubt die Verwendung des keyIdentifiers eine größere Flexibilität zum Auffinden eines Zertifizierungspfades.

(Außerdem müssen die Zertifikate, die den keyIdentifier in der authorityKeyIdentifier-Erweiterung besitzen, nicht zurückgezogen werden, wenn die CA sich bei gleichbleibendem Schlüssel ein neues Zertifikat ausstellen lässt.)

3. Überprüfung von Sperrlisten

Zu jedem Aussteller-Zertifikat kann dem IPSec Client die zugehörige CRL (Certificate Revocation List) zur Verfügung gestellt werden. Sie wird in das Windows-Verzeichnis \ncple\crls\ gespielt. Ist eine CRL vorhanden, so überprüft der IPSec Client eingehende Zertifikate daraufhin, ob sie in der CRL geführt sind. Gleiches gilt für eine ARL (Authority Revocation List), die in das Windows-Verzeichnis \ncple\arls\ gespielt werden muss.

Sind eingehende Zertifikate in den Listen von CRL oder ARL enthalten, wird die Verbindung nicht zugelassen.

Sind CRLs oder ARLs nicht vorhanden findet keine diesbezügliche Überprüfung statt.

4.1.10 Firewall-Einstellungen

Die Firewall-Einstellungen können für alle Netzwerkadapter wie auch für RAS-Verbindungen genutzt werden. Die aktivierte Firewall wird in der grafischen Oberfläche des Clients als Symbol (Mauer mit Pfeil) dargestellt. Grundsätzliche Aufgabe einer Firewall ist es, zu verhindern, dass sich Gefahren aus anderen bzw. externen Netzen (Internet) in das eigene Netzwerk ausbreiten. Deshalb wird eine Firewall auch am Übergang zwischen Firmennetz und Internet installiert. Sie prüft alle ein- und ausgehenden Datenpakete und entscheidet auf der Basis vorher festgelegter Konfigurationen, ob ein Datenpaket durchgelassen wird oder nicht. Die hier zu aktivierende Firewall arbeitet nach dem Prinzip der Stateful Inspection. Sicherheit wird dabei in zweierlei Hinsicht gewährleistet. Zum einen verhindert diese Funktionalität den unbefugten Zugriff auf Daten und Ressourcen im zentralen Datennetz. Zum anderen überwacht sie als Kontrollinstanz den jeweiligen Status aller bestehenden Internet-Verbindungen. Die Stateful Inspection Firewall erkennt darüber hinaus, ob eine Verbindung "Tochterverbindungen" geöffnet hat – wie beispielsweise bei FTP oder Netmeeting – deren Pakete ebenfalls weitergeleitet werden müssen. Für die Kommunikationspartner stellt sich eine Stateful Inspection-Verbindung als eine direkte Leitung dar, die nur für einen den vereinbarten Regeln entsprechenden Datenaustausch genutzt werden darf (siehe → Handbuch, Beispiele und Erklärungen).

Parameter:

- ☐ Stateful Inspection aktivieren
- ☐ Ausschließlich Kommunikation im Tunnel zulassen
- ☐ NetBIOS über IP zulassen
- ☐ Bei Verwendung des Microsoft DFÜ-Dialers ausschließlich Kommunikation im Tunnel zulassen

Stateful Inspection aktivieren

aus: Die Sicherheitsmechanismen der Firewall werden nicht in Anspruch genommen.

immer: Die Sicherheitsmechanismen der Firewall werden immer in Anspruch genommen, d.h. auch wenn keine Verbindung aufgebaut ist, ist der PC vor unberechtigten Zugriffen geschützt.

bei bestehender Verbindung: Der PC ist dann nicht angreifbar, wenn eine Verbindung besteht.

Ausschließlich Kommunikation im Tunnel zulassen

Ausschließlich Kommunikation im Tunnel zulassen: Bei aktivierter Firewall kann diese Funktion zusätzlich eingeschaltet werden, um in ein- und ausgehender Richtung ausschließlich VPN-Verbindungen zuzulassen.

NetBIOS über IP zulassen

Mit diesem Parameter wird ein Filter aufgehoben, der Microsoft NetBios Frames unterdrückt. Diesen Filter aufzuheben, um den Verkehr von NetBios Frames zu gestatten, ist immer dann zweckmäßig, wenn Sie zum Beispiel Microsoft Networking über den IPSec Client nutzen.

In der Standardeinstellung ist dieser Filter gesetzt, das heißt der Checkbutton nicht mit einem Haken markiert, so dass Microsoft NetBios Frames unterdrückt werden, damit sie den Datenverkehr nicht unnötig belasten. Markieren Sie den Checkbutton mit einem Haken, werden NetBios Frames over IP erlaubt.

Bei Verwendung des Microsoft DFÜ-Dialers ausschließlich Kommunikation im Tunnel zulassen

Bei Verwendung des Client-Monitors wird bei Aktivierung dieser Funktion verhindert, dass eine Kommunikation über den DFÜ-Dialer zum Internet stattfinden kann.

5. Verbindungsaufbau

Um die Einstellungen Ihres IPSec Clients auf Funktionstüchtigkeit hin zu überprüfen, bietet Bintec einen entsprechenden öffentlichen Testzugang. Eine detaillierte Konfigurationsanleitung zur Nutzung dieses VPN-Testzugangs in Verbindung mit dem Bintec Secure IPSec Client finden Sie unter www.bintec.de.

■ Verbindungsaufbau zum Zielsystem

Sobald die Software installiert und ein Profil korrekt konfiguriert wurden, kann die Anwahl über das Profil an das Zielsystem stattfinden. Dabei ist auch die Art der Anwahl Bestandteil der Konfiguration eines Profils. Sie können aus drei Anwahl-Modi für den Verbindungsaufbeu wählen: automatisch, manuell und wechselnd. Sie definieren den Modus des Verbindungsaufbaus zu einem Zielsystem in der Profil-Einstellungen unter “Verbindungsaufbau” im Parameterfeld “Line Management”.

Automatischer Verbindungsaufbau:

Im Unterschied zu Microsoft RAS, bei dem jedes Ziel manuell angewählt werden muss, arbeitet die Client Software nach dem Prinzip der LAN-Emulation. Dabei ist es lediglich erforderlich, die entsprechende Applikations-Software zu starten (Email, Internet Browser, Terminal Emulation, etc.). Die Verbindung wird dann, entsprechend den Parametern des Zielsystems, automatisch aufgebaut und gehalten.

Manueller Verbindungsaufbau:

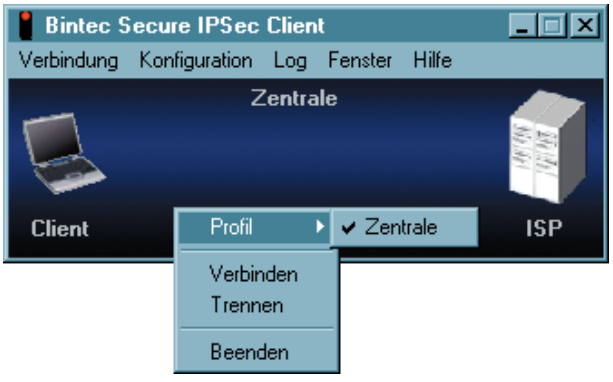
Daneben ist es auch möglich manuell die Verbindung zu einem ausgewählten Ziel herzustellen, indem Sie im Monitor “Verbindung” anklicken und “Verbinden” wählen.

Wechselnder Verbindungsaufbau:

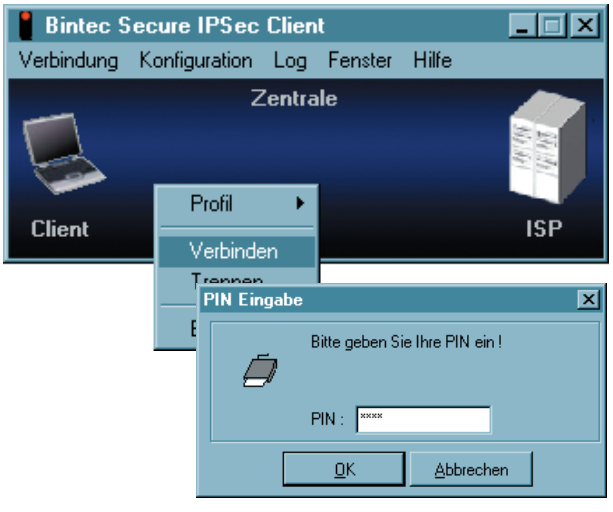
Wird dieser Modus gewählt, muss zunächst die Verbindung “manuell” aufgebaut werden. Danach wechselt der Modus je nach Verbindungsabbau wie folgt:
– Wird die Verbindung mit Timeout beendet, so wird die Verbindung bei der nächsten Anforderung “automatisch” hergestellt,
– wird die Verbindung “manuell” abgebaut, muss sie auch wieder “manuell” aufgebaut werden.

■ Verbinden

Gleich wie die Verbindung aufgebaut wird, der Monitor, sofern er im Vordergrund sichtbar ist, zeigt immer den Status des Verbindungsaufbaus wie in folgendem Beispiel an:

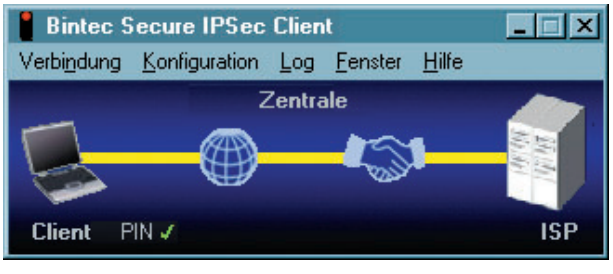


Zunächst wird das Zielsystem ausgewählt – hier über das Menü, das nach einem rechten Mausklick erscheint.

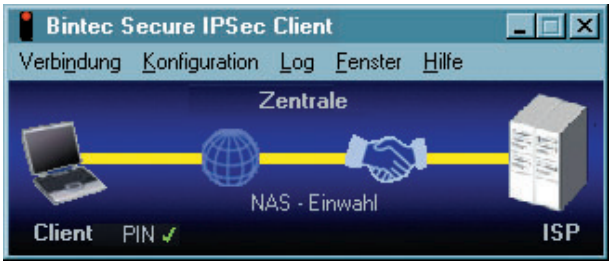


Danach wird die Verbindung hergestellt – hier manuell über das Menü, das nach dem rechten Mausklick erscheint.

Wurde die Verwendung eines (Soft-)Zertifikats konfiguriert – wie bei der Testverbindung mit SSL – so muss zunächst die PIN eingegeben werden.



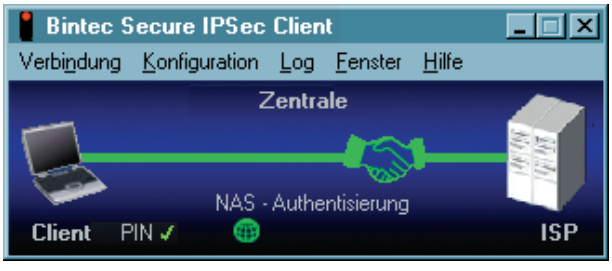
Anschließend wird eine Verbindung zum Internet Service Provider (ISP) hergestellt (gelbe Linie). Die Einwahl dorthin wird nun mit einem Globus, die Authentisierung beim ISP als Händeschütteln dargestellt. Dabei wechseln die Farben der Symbole je nach aktuellem Status:



hellblau = Station des Verbindungsaufbaus

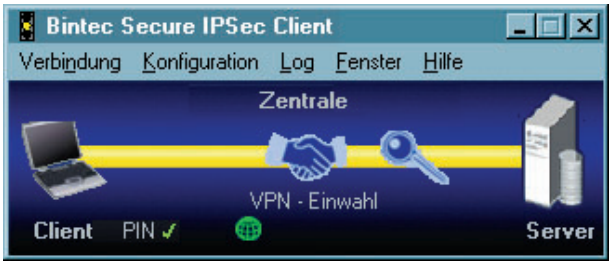
dunkelblau = Station wird gerade durchlaufen

grün = Station erfolgreich durchlaufen (links der Globus)

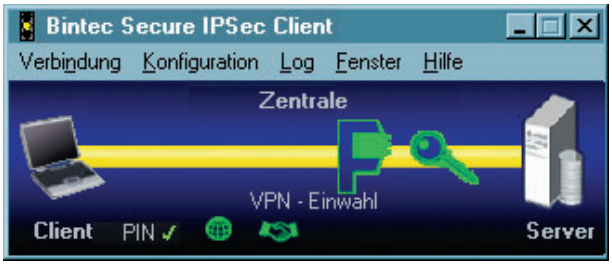


Die erfolgreich durchlaufenen Stationen werden als verkleinerte Symbole dargestellt.

Nach der Verbindung zum ISP (grüne Linie) und der Authentisierung am Network Access Server (grünes Händeschütteln)



... wird der Tunnel aufgebaut (gelbe, dicke Linie) und die Einwahl am Server (VPN Gateway) beginnt. Auch hier muss eine Authentisierung stattfinden. Die Verschlüsselung (der IPSec-Richtlinie) wird mit einem Schlüssel angezeigt.



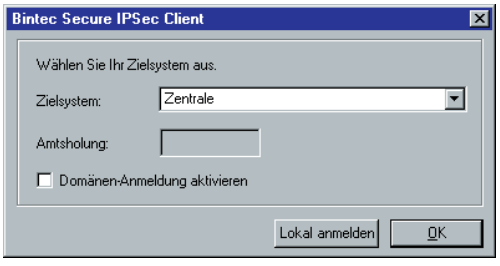
Wenn die Konfiguration der Gegenstelle darauf eingestellt ist, kann auch Kompression konfiguriert werden.

Ist die letzte Station des Verbindungsaufbaus (hier die Verschlüsselung) durchlaufen, schaltet das Ampellicht auf grün wie auch anschließend die Tunnelverbindung. Die Verbindung ist damit hergestellt!

Beachten Sie, dass grüne Ampellampen eine stehende Verbindung und anfallende Gebühren signalisieren!

Client Logon

Erfolgt das Client Logon am Network Access Server vor dem Windows Logon an der remote Domäne, indem die Logon Optionen genutzt werden (siehe → Monitor, Logon Optionen), so erfolgt der Verbindungsaufbau prinzipiell genau so, wie oben unter "Verbinden" beschrieben.

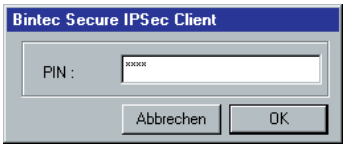


Nach der Auswahl des Zielsystems wird mit Klick auf den OK-Button der Verbindugsaufbau eingeleitet.

Lokal anmelden:
Ein Klick auf diesen Button bricht den Dialog zum Verbindungsaufbau ab.

Domänen-Anmeldung aktivieren:

Mit dieser Option ist eine sichere WAN-Domänen-Anmeldung möglich, auch wenn vorher keine ordnungsgemäße Abmeldung erfolgte. Die Anmeldung dauert einige Sekunden. Diese Funktion wird nicht benötigt, wenn bei einem ordnungsgemäßen Herunterfahren (Shut Down) des Computers eventuell gemappte Laufwerke korrekt getrennt wurden.
(Diese Option ist nur bei einem NT-Server als Gegenstelle einsetzbar.)



Wurde die Verwendung eines (Soft-)Zertifikats konfiguriert, so muss zunächst die PIN eingegeben werden.

Die weiteren Stationen des Verbindungsaufbaus erfolgen genau so, wie oben unter "Verbinden" beschrieben ...

... bis die Verbindung steht.

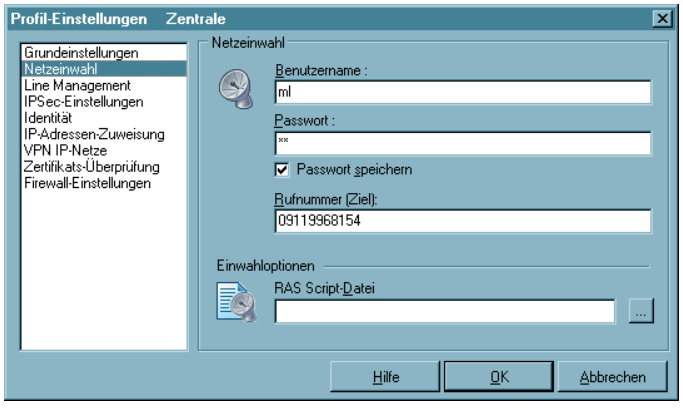
Passwörter und Benutzernamen

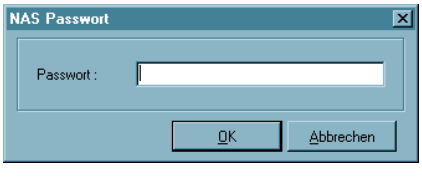
Das Passwort (siehe → Netzeinwahl, Passwort) benötigen Sie, um sich gegenüber dem Network Access Server (NAS) ausweisen zu können, wenn die Verbindung aufgebaut ist. Das Passwort darf bis zu 254 Zeichen lang sein. Für gewöhnlich wird Ihnen ein Passwort vom Zielsystem zugewiesen, da Sie vom Zielsystem auch erkannt werden müssen. Sie erhalten es von Ihrem Stammhaus, vom Internet Service Provider oder dem Systemadministrator. Wenn Sie das Passwort eingeben, werden alle Zeichen als Stern (*) dargestellt, um sie vor ungewünschten Beobachtern zu verbergen. Es ist wichtig, dass Sie das Passwort genau nach der Vorgabe eintragen und dabei auch auf Groß- und Kleinschreibung achten.

Auch wenn Sie für den Verbindungsaufbau “automatisch“ gewählt haben (siehe oben → Verbindungsaufbau zum Zielsystem), müssen Sie die Verbindung beim ersten Mal manuell aufbauen und das Passwort eingeben. Für jeden weiteren automatischen Verbindungsaufbau wird das Passwort selbständig übernommen, bis der PC erneut gebootet oder das Zielsystem gewechselt wird. D.h. für eine Reihe von “automatischen” Verbindungsaufbaus wird das Passwort nach der ersten Eingabe und dem ersten Verbindungsaufbau selbständig übernommen, auch wenn die Funktion “Passwort speichern” (siehe → Netzeinwahl) nicht aktiviert wurde. Erst ein Boot-Vorgang löscht das einmal eingegebene Passwort. (Beachten Sie dazu auch → Logon Optionen).

Soll das Passwort mit dem Booten nicht gelöscht werden, so muss die Funktion “Passwort speichern” aktiviert werden (siehe → Netzeinwahl). Bitte beachten Sie dabei, dass im Falle gespeicherter Passwörter, jedermann mit Ihrer Client Software arbeiten kann – auch wenn er die Passwörter nicht kennt.

Passwort für NAS-Einwahl

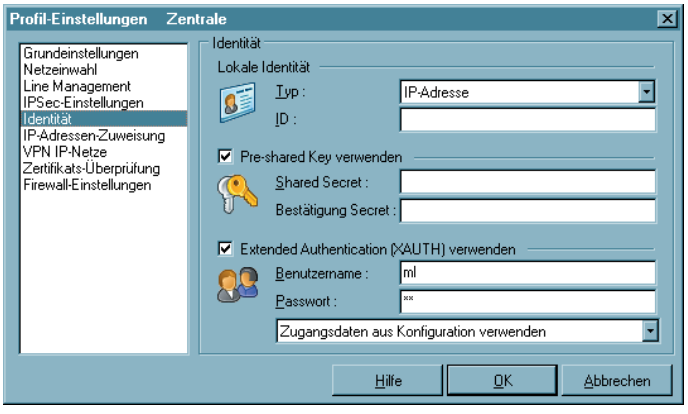




Wird das Passwort für die NAS-Einwahl nicht eingegeben oder nicht gespeichert, so wird es bei einem Verbindungsaufbau in einem eigenen Dialog abgefragt.

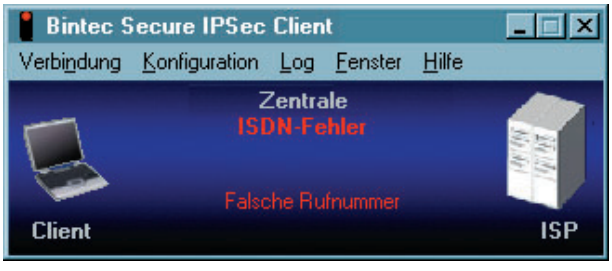
Der “Benutzername” für die Netzeinwahl muss immer in der Konfiguration für das Ziel eingegeben werden. Ohne ihn kann keine Einwahl an den NAS erfolgen. (Siehe → Profil-Einstellungen, Netzeinwahl)

Benutzername und Passwort für Extended Authentication



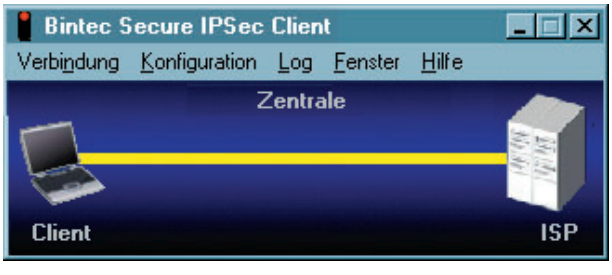
Wird Extended Authentication eingesetzt, so müssen Benutzername und Passwort in der Konfiguration des Pofils eingegeben werden, sonst findet kein Verbindungsaufbau statt (siehe → Profil-Einstellungen, Identität, Extended Authentication (XAUTH) verwenden).

Verbindungsabruch und Fehler



Ereignet sich ein Fehler, so wird die Verbindung nicht hergestellt und die Fehlerursache im Monitor angezeigt (beachten Sie dazu den Abschnitt “Fehler- und ISDN-Meldungen”).

Trennen

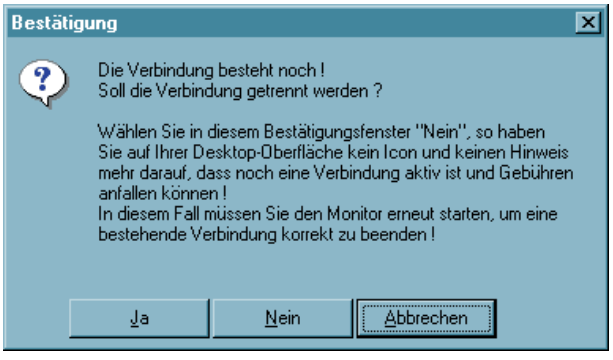


Mit der Funktion “Trennen“ wird der Abbau der aktuell bestehenden Verbindung manuell durchgeführt. Wenn Sie die Möglichkeit behalten wollen, jederzeit die Verbindung manuell abbauen zu können, setzen Sie den Verbindungsaufbau auf “manuell” und deaktivieren den automatischen Timeout, indem Sie ihn auf Null (0) setzen (→ Verbindungsaufbau).

Wenn die Verbindung abgebaut wird, wechselt die farbliche Darstellung der Verbindungslinie bis sie verschwindet und die Ampellampen des Monitors für die gesamte Offline-Dauer von grün zu rot.

Trennen und Beenden des Monitors

Besteht eine Verbindung noch, und wird der Monitor beendet, so wird nicht automatisch die Verbindung getrennt. Soll die möglicherweise kostenpflichtige Verbindung bestehen bleiben, obwohl der Monitor beendet wird, so wird dazu ausdrücklich eine Bestätigung von der Software verlangt (siehe Bild unten).



Klicken Sie in diesem Bestätigungsfenster auf “Nein”, so haben Sie auf Ihrer Desktop-Oberfläche kein Icon und keinen Hinweis mehr darauf, dass noch eine Verbindung aktiv ist und Gebühren anfallen können! In diesem Fall müssen Sie den Monitor erneut starten, um eine bestehende Verbindung korrekt zu beenden!

6. Beispiele und Erklärungen

In diesem Abschnitt des Handbuchs werden einige Grundbegriffe des Routings und des IPSec-Verkehrs erklärt. Anhand von Beispielen wird die Konfiguration des IPSec Clients für bestimmte Funktionalitäten dargestellt.

6.1 IP-Funktionen

Um ein IP-Netzwerk korrekt zu konfigurieren, müssen die Regeln der IP-Adressierung eingehalten werden. Untenstehend sind einige Richtlinien und Terminologien aufgeführt. Zu weiteren Informationen über IP-Netzwerke wird entsprechende Fachliteratur empfohlen.

6.1.1 Geräte eines IP-Netzwerks

IP-Adressen werden den Schnittstellen der Geräte eines IP-Netzwerks zugewiesen. Diese Geräte werden auch als Hosts oder Rechner bezeichnet. Mehrfach vernetzten Geräten (z.B. Router) können auch mehrere Adressen zugeordnet werden. Der Begriff Host-Adresse bezeichnet die IP-Adresse des Rechners eines IP-Prozesses, unabhängig von der tatsächlichen physikalischen Struktur des Geräts oder der Schnittstellen.

6.1.2 IP-Adress-Struktur

IP-Adressen haben eine Länge von vier Oktetten, 32 Bits (4 Bytes), und werden in dezimaler oder hexadezimaler Schreibweise mit Punkt "." getrennt notiert. Zum Beispiel:

```
198.10.6.27 oder
C6.0A.06.1B oder
0xC6.0x0A.0x06.0x1B
```

Die Adressen werden getrennt in einen Netzwerk-Abschnitt, der das zugehörige Netz adressiert, und eine lokale Adresse, dem sogenannten "Restfeld" (auch Host-Abschnitt), der das jeweilige Gerät innerhalb des Netzwerks adressiert. Alle Geräte innerhalb eines einzelnen Netzwerks haben denselben Netzwerk-Abschnitt gemeinsam. Jedes Gerät (Host) hat dabei sein eigenes Restfeld.

Es gibt drei Klassen von Internet-Adressen, je nachdem wieviele Bytes der IP-Adresse für Netzwerk-Abschnitt und Restfeld verwendet werden.

Klasse (Class) A, große Netzwerke: Netzwerknummern 1 - 127

Bei Adressen der Klasse A ist das höchste Bit gleich Null, die nächsten sieben Bits entsprechen dem Netzwerk und die verbleibenden 24 Bits der lokalen Adresse.

Netzwerk-Abschnitt beansprucht 1 Byte (max. 126 unterschiedliche Netzwerke)

Restfeld beansprucht 3 Bytes (max. 2 hoch 24 = 16.777.216 verschiedene Geräte)

Damit können max. 127 unterschiedliche Netzwerke, jedes mit max. 16.777.216 verschiedenen Geräten, adressiert werden.

Klasse (Class) B, mittlere Netzwerke: Netzwerknummern 128 - 191

Bei Adressen der Klasse B haben die beiden höchsten Bits die Werte 1 und 0, die nächsten 14 Bits entsprechen dem Netzwerk und die verbleibenden 16 Bits der lokalen Adresse.

Netzwerk-Abschnitt beansprucht 2 Byte (max. 16.384 unterschiedliche Netzwerke)

Restfeld beansprucht 2 Bytes (max. 2 hoch 16 = 65.536 verschiedene Geräte)

Damit können max. 16.384 unterschiedliche Netzwerke, jedes mit max. 65.526 verschiedenen Geräten, adressiert werden.

Klasse (Class) C, kleine Netzwerke: Netzwerknummern 192 - 223

Bei Adressen der Klasse C haben die drei höchsten Bits die Werte 1, 1 und 0, die folgenden 21 Bits entsprechen dem Netzwerk und die letzten 8 Bits der lokalen Adresse.

Netzwerk-Abschnitt beansprucht 3 Bytes (max. 2.097.152 unterschiedliche Netzwerke)

Restfeld beansprucht 1 Byte (max. 256 verschiedene Geräte)

Damit können max. 2.097.152 unterschiedliche Netzwerke, jedes mit max. 256 verschiedenen Geräten, adressiert werden.

Beispiel:

```
           Netz    Host
Klasse A: 122. | 087.    156.    045
Klasse B: 162.   143. | 085.    132
Klasse C: 195.   076.   212. | 024
```

Bitte beachten Sie bei der Adressvergabe, dass für einen einzelnen physikalischen Rechner mehrere IP-Adressen verwendbar sein müssen. Eine Workstation kann mit einer IP-Adresse auskommen. Ein Router benötigt für jede seiner Schnittstellen eine IP-Adresse, mindestens jedoch zwei – eine für den Anschluss zum lokalen Netz (LAN IP-Adresse), eine für den Anschluss zur WAN-Seite.

6.1.3 Netzmasken (Subnet Masks)

In einem Wide Area Network können verschiedene, physikalisch getrennte Netze (LANs) dem gleichen Netzwerk (WAN) mit der gleichen Netzwerknummer angehören. Anhand dieser Netzwerknummer allein kann kein Router entscheiden, ob er bei einer IP-Kommunikation eine Verbindung zu einem physikalisch anderen Netz innerhalb des WANs aufbauen soll. Das Netzwerk (WAN) muss daher in kleinere Abschnitte (LANs) unterteilt werden, die einen eigenen Adressblock erhalten. Jeder Adressblock der einzelnen physikalischen Netze wird als Subnet bezeichnet. Durch diese Unterteilung eines Netzwerks in Subnets wird die Hierarchie aus Netzwerk und Rechner zu einer Hierarchie erweitert aus Netzwerk, Subnet und Rechner.

Diese erweiterte Hierarchie erleichtert zum einen das Auffinden eines Rechners im Gesamtnetz (WAN). Man kann sich dies vorstellen analog zur Nomenklatur im Telefonnetz, wo zum Beispiel die Ortsvorwahl aussagt in welchem Bereich sich ein Anschluss befindet. Diese Hierarchie gewährt auch eine gewisse Zugriffssicherheit. So kann in einem Firmennetz zum Beispiel der Rechner eines Subnets nicht ohne weiteres auf Ressourcen eines anderen Subnets zugreifen – etwa ein Mitarbeiter aus der Fertigungsabteilung auf Datenbestände aus der Personalabteilung – wenn die Netz-Masken nach Firmenabteilungen entsprechend gewählt sind.

Die Netz-Maske (Subnet Mask) gibt den Standort des Subnet-Felds in einer IP-Adresse an. Die Netz-Maske ist eine binäre 32-Bit-Zahl wie eine IP-Adresse. Sie hat eine “1” an allen Stellen des Netzwerk-Abschnitts der IP-Adresse (je nach Netzwerk-Klasse innerhalb des ersten bis dritten Oktetts). Das darauf folgende Oktett gibt die Position des Subnet-Feldes an. Die im Subnet-Feld an den Netzwerk-Abschnitt aufschließenden Einsen geben die Subnet-Bits an. Alle übrigen Stellen mit ”0” verbleiben für den Host-Abschnitt.

■ Beispiele

Beispiel 1:

Die Netzmaske dient der Interpretation der IP-Adresse. So kann eine Adresse 135.96.7.230 mit der Maske 255.255.255.0 so interpretiert werden: Das Netzwerk hat die Adresse 135.96.0.0, das Subnet hat die Nummer 7, der Rechner Nummer 230. Eine IP-Adresse mit 135.96.4.190 gehört dem gleichen Netzwerk aber einem anderen Subnet (4) an.

Binäre Darstellung:

```
135.96.7.230     = 10000111 11000000 | 00000111 | 11100110
135.96.4.190     = 10100000 10010101 | 00000100 | 10111110
255.255.255.0    = 11111111 11111111 | 11111111 | 00000000
                   Netzwerk          | Subnet   |
255.255.248.0    = 11111111 11111111 | 11111|000  00000000
```

Hätte die Netz-Maske in obigem Beispiel nicht den Standardwert 255.255.255.0, sondern 255.255.248.0, befänden sich die IP-Adressen im gleichen Subnet – und Routing würde nicht stattfinden.

Beispiel 2:

Zwei IP-Adressen mit 160.149.115.8 und 160.149.117.201 und der Netz-Maske 255.255.252.0 befinden sich im gleichen Netzwerk 160.149, gehören aber unterschiedlichen Subnets an.

Binäre Darstellung:

```
160.149.115.8    = 10100000 10010101 | 011100|11 00001000
160.149.117.201  = 10100000 10010101 | 011101|01 11001001
255.255.252.0    = 11111111 11111111 | 111111|00 00000000
                   Netzwerk          | Subnet|
```

Die Wahl einer geeigneten Netzmaske hängt von der Netzwerk-Klasse, der Beschaffenheit der möglichen Subnets, ihrer Anzahl und ihrem Wachstum ab. Ziehen Sie zur Planung einschlägige Tabellen oder einen Subnet-Taschenrechner zu Rate.

Subnet-Tabelle Klasse C:

Subnet-Bits	Host-Bits	Netz-Maske	Subnets	Rechner
2	6	255.255.255.192	2	62
3	5	255.255.255.224	6	30
4	4	255.255.255.240	14	14
5	3	255.255.255.248	30	6
6	2	255.255.255.252	62	2

(Berechnung: 2 hoch n minus 2 = Anzahl der Subnets/Rechner
n: Anzahl der Subnet/Host-Bits)

Mit einer Netz-Maske 255.255.255.240 wird ein Netz der Klasse C in Subnets geteilt. Mit dieser Netz-Maske sind insgesamt 14 Subnets mit jeweils max. 14 Rechnern möglich.

```
255.255.255.240  11111111 11111111 11111111 | 1111 | 0000
199.  9. 99.130  11000111 00001001 01100011 | 1000 | 0010  Subnet-Nummer 8
199.  9. 99.146  11000111 00001001 01100011 | 1001 | 0010  Subnet-Nummer 9
                 Netzwerk                   |Subnet| Host
```

■ Standard-Masken

Netzmaske für Klasse A: 255. 0. 0. 0

Netzmaske für Klasse B: 255. 255. 0. 0

Netzmaske für Klasse C: 255. 255. 255. 0

Reservierte Adressen

Einige IP-Adressen dürfen Geräten eines Netzwerks nicht zugeordnet werden. Dazu gehören die Netzwerk- oder Subnet-Adresse und die Rundsendungsadresse für Netzwerke bzw. Subnets. Netzwerk-Adressen bestehen aus der Netzwerknummer und dem Host-Feld, das mit binären Nullen gefüllt ist (z.B. 200.1.2.0, 162.66.0.0., 10.0.0.0) – auch Loop Back, es findet keine Übertragung ins Netzwerk statt. Die Rundsendungsadresse eines Netzwerks besteht aus der Netzwerknummer und dem Host-Feld mit binären Einsen (z.B. 200.1.2.255, 162.66.255.255., 10.255.255.255) – daher auch "All One Broadcast", alle Stationen eines Netzwerks werden adressiert.

Beispiel:

198.10.2.255	adressiert alle Stationen im Netz 198.10.2.
255.255.255.255	adressiert alle Stationen in allen angeschlossenen Netzen
0.0.0.0	All Zero Broadcast: Ungültige Adresse.

Bitte beachten Sie, dass diese Adresse oft für Standard-Einstellungen benutzt wird.

6.1.4 Zum Umgang mit IP-Adressen

- ☐ Jede IP-Adresse im unternehmensweiten Netz sollte nur einmalig vorhanden sein. Beachten Sie dies bei Internet-Anschluss und Anschluss neuer Netze.
- ☐ Benutzen Sie ein nachvollziehbar logisches Schema bei der Adress-Vergabe, z.B. Verwaltungseinheiten, Gebäude, Abteilungen etc.
- ☐ Für den Anschluss ans Internet benötigen Sie eine offizielle einmalige Internet-Adresse.
- ☐ Vergeben Sie, wenn möglich, keine IP-Adresse, deren Netzwerk- oder Host-Abschnitt mit "0" endet. Dies könnte zu Fehlinterpretationen und undefinierbaren Fehlern im Netz führen.
- ☐ Netzmasken werden vom Internet-Protokoll nur ausgewertet, wenn die Netzwerknummern der Kommunikationspartner gleich sind.
- ☐ Wie die Adress-Klassen haben auch die Netz-Masken unterschiedlich lange Netzwerk-Abschnitte.

6.2 Security

Im Parameterfeld “IPSec-Einstellungen” der Profil-Einstellungen sind die Konfigurationsparameter zu IPSec für den Einsatz in Remote Access-Umgebungen gesammelt. Im folgenden wird auf einige Konfigurationsmöglichkeiten Bezug genommen.

6.2.1 IPSec – Übersicht

IPSec kann nur für IP-Datenverkehr eingesetzt werden. Die IPSec-Spezifikation umfasst nicht nur das (Layer 3-) Tunneling, sondern auch alle notwendigen Sicherheitsmechanismen, wie starke Authentisierung, Schlüsselaustausch und Verschlüsselung.

Mit den IPSec RFCs (2401 - 2409) lässt sich ein VPN mit vorgegebener Security für IP realisieren. Tunneling und Security sind für IPSec vollständig beschrieben, so dass ein komplettes Rahmenwerk für das VPN zur Verfügung steht. Prinzipiell ist es möglich, herstellerunabhängige veschiedene Komponenten zu nutzen. In Site to Site VPNs etwa könnten die VPN Gateways von veschiedenen Herstellern stammen, in End to Site VPNs könnten die Clients von einem anderen Hersteller als die Gateways sein.

Der Verbindungsaufbau zum IPSec-Verkehr erfolgt auf Basis des Internet Key Exchange-Protokolls (IKE).

■ IPSec – allgemeine Funktionsbeschreibung

In jedem IP-Host (Client oder Gateway) der IPSec unterstüzt, gibt es ein IPSec-Modul, bzw. eine IPSec-Maschine. Dieses Modul untersucht jedes IP-Paket nach bestimmten Eigenschaften, um die jeweils entsprechende Security-Behandlung darauf anzuwenden.

Die Prüfung der vom IP Stack ausgehenden IP-Pakete erfolgt bezüglich einer Secure Policy Database (SPD). Dabei werden alle konfigurierten SPDs abgearbeitet. (Bei Einsatz des IPSec Clients werden die SPDs nur zentralseitig am Gateway gehalten.)

Die SPD besteht aus mehreren Einträgen (SPD Entries), die wiederum einen Filterteil beinhalten. Der Filterteil (siehe → Erweiterte Firewall-Einstellungen) oder Selektor eines SPD-Eintrags besteht hauptsächlich aus IP-Adressen, UDP und TCP Ports sowie anderer IP Header-spezifischer Einträge. Wenn Werte eines IP-Pakets mit Werten aus dem Selektorteil des SPD-Eintrags übereinstimmen, wird aus den SPD-Einträgen weiter ermittelt, wie mit diesem IP-Paket zu verfahren ist. Das Paket kann einfach durchgelassen werden (permit), es kann abgelehnt bzw. weggeworfen werden (deny) oder bestimmte Security-Richtlinien des IPSec-Prozesses kommen an ihm zur Anwendung. Diese Security-Richtlinien stehen auch im SPD-Eintrag beschrieben.

Wird auf diese Weise festgestellt, dass ein IP-Paket mit einem SPD-Eintrag verknüpft ist, der einen IPSec-Prozess einleitet, so wird überprüft, ob bereits eine Sicherheits-Verknüpfung (Security Association, SA) für diesen SPD-Eintrag existiert. Existiert

noch keine SA, wird vor dem Aushandeln einer SA zunächst eine Authentisierung und ein Schlüsselaustausch (siehe unten → IPSec-Verhandlung Phase 1) vorgenommen.

Nach der SA-Verhandlung erfolgen in einem weiteren Schritt (siehe unten → IPSec-Verhandlung Phase 2) die Verhandlungen für eine Verschlüsselung (ESP) und/oder Authentisierung (AH) der Datenpakete.

Die SA beschreibt, welches Sicherheitsprotokoll verwendet werden soll. ESP (Encapsulating Security Payload) unterstützt die Verschlüsselung und die Authentisierung von IP-Paketen, AH (Authentication Header) unterstüzt nur die Authentisierung von IP-Paketen. Die SA beschreibt auch, in welcher Betriebsart das Sicherheitsprotokoll benutzt werden soll (Tunnel- oder Transportmodus). Im Tunnelmodus wird ein IP Header hinzugefügt, im Transportmodus wird der Original-Header verwendet. Weiter beschreibt die SA, welcher Algorithmus zur Authentisierung verwendet werden soll, welche Verschlüsselungsmethode (bei ESP) und welcher Schlüssel zur Anwendungen kommen sollen. Die Gegenstelle muss selbstverständlich nach der gleichen SA arbeiten.

Ist die SA ausgehandelt, wird jedes Datenpaket gemäß Betriebsmodus (Tunnel oder Transport) und Protokoll (ESP oder AH) bearbeitet. Der IPSec Client nutzt immer das ESP-Protokoll im Tunnelmodus.

6.2.2 Erweiterte Firewall-Einstellungen / Extended Firewall Settings

Die erweiterten Firewall-Einstellungen bestehen hauptsächlich aus IP-Adressen, UDP und TCP Ports sowie anderer IP Header-spezifischer Einträge. Wenn Werte eines IP-Pakets mit Werten aus dem Selektorteil des Regel-Eintrags übereinstimmen, wird aus den Regel-Einträgen weiter ermittelt, wie mit diesem IP-Paket zu verfahren ist.

Im folgenden die Einträge zur Konfiguration im IPSec Client:

☐ Ausführung / Command

gestatten (permit), sperren (deny), inaktiv (disabled)

☐ IP-Protokoll / IP Protocol

Dies ist das Transportprotokoll (ICMP, TCP oder UDP). Eines der angebotenen Protokolle kann ausgewählt werden oder ein beliebiges (alle / any) wird genutzt.

☐ IP-Adresse (Quelle) / Source IP Address

Dies kann eine einfache IP-Adresse oder ein Adressbereich sein. Letzteres ist nötig, wenn mehrere Ausgangssysteme mit einer gemeinsamen SA unterstützt werden sollen (z.B. hinter einer Firewall).

☐ IP-Adresse (Ziel) / Destination IP Address

Dies kann eine einfache IP-Adresse oder ein Adressbereich sein. Letzteres ist nötig, wenn mehrere Zielsysteme mit einer gemeinsamen SA unterstützt werden sollen (z.B. hinter einer Firewall).

☐ Port (Quelle) / Source Port

Dies können einzelne TCP- oder UDP-Portnummern oder ein Bereich von Portnummern sein. Die Portnummern mit zugeordnetem Service bestimmen Sie über den Auswahlbutton [...].

☐ Port (Ziel) / Destination Port

Dies können einzelne TCP- oder UDP-Portnummern oder ein Bereich von Portnummern sein. Die Portnummern mit zugeordnetem Service bestimmen Sie über den Auswahlbutton [...].

6.2.3 SA-Verhandlung und Richtlinien / Policies

Damit der IPSec-(Filter-)Prozess in Gang kommen kann, müssen vorher verschiedene SAs verhandelt worden sein. Es wird eine SA für Phase 1 (IKE-Richtlinie) sowie mindestens zwei (je für ein- und ausgehende Verbindung) für Phase 2 (IPSec-Richtlinie) ausgehandelt. [Für jedes Zielnetz (siehe → Profil-Einstellungen, VPN Networks) werden ebenfalls zwei SAs ausgehandelt.]

- **Phase 1 (Parameter der IKE-Richtlinie / IKE Policy):**

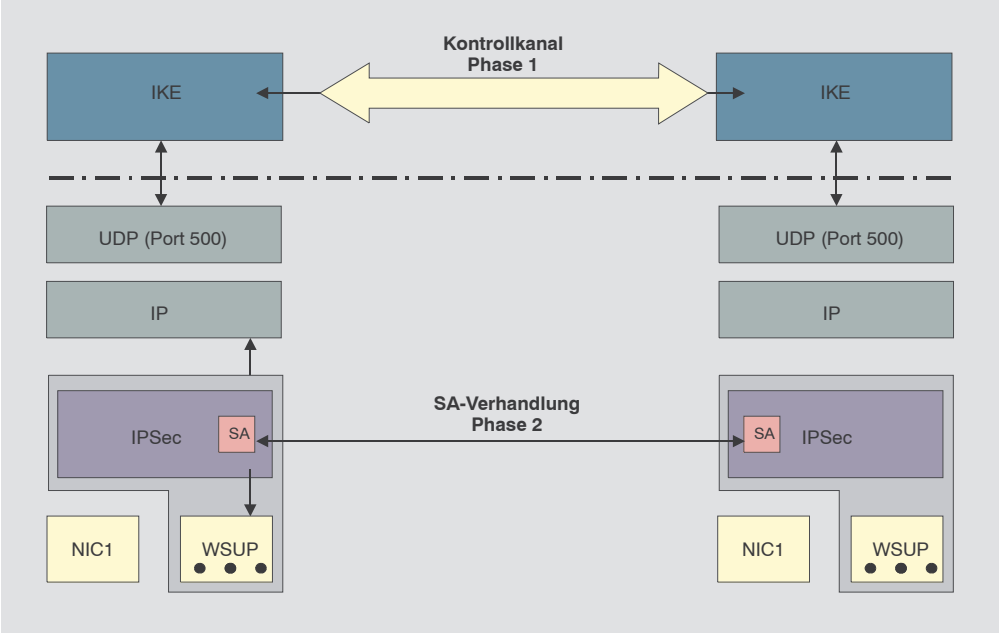
  Der Kontrollkanal wird im Tunnelmodus von IPSec über das IKE-Protokoll zur IP-Adresse des Gateways aufgebaut, im Transportmodus direkt zur IP-Adresse der Gegenstelle.

  Parameter zur Festlegung von Verschlüsselungs- und Authentisierungsart über das IKE-Protokoll definieren Sie in den IKE-Richtlinien. Dabei kann die Authentisierung über einen Pre-shared Key oder eine RSA Signatur erfolgen. (Entsprechende Richtlinien sind im Richtlinien-Editor vorkonfiguriert.)

- **Phase 2 (Parameter der IPSec-Richtlinie / IPSec Policy):**

  Die SA-Verhandlung wird über den Kontrollkanal abgewickelt. Von der IPSec-Maschine wird die SA an das IKE-Protokoll übergeben, das sie über den Kontrollkanal zur IP-Sec-Maschine der Gegenstelle überträgt.

Kontrollkanal und SA-Verhandlung



Bildbeschreibung:

Damit der IPSec-Prozess in Gang kommen kann, muss vorher die SA verhandelt worden sein. Diese SA-Verhandlung findet pro SPD – die für verschiedene Ports, Adressen und Protokolle angelegt sein können – einmal statt. Für diese SA-Verhandlung wird ein Kontrollkanal benötigt.

Im Client muss nun zunächst eine Layer 2-(PPP)-Verbindung zum Provider hergestellt werden. Dabei bekommt er (bei jeder Einwahl) eine neue IP-Adresse. Das IPSec-Modul im Client bekommt ein IP-Paket mit der Zieladresse der Firmenzentrale. Ein SPD-Eintrag für dieses IP-Paket wird gefunden aber es existiert noch keine SA. Das IPSec-Modul stellt die Anforderung an das IKE-Modul, eine SA auszuhandeln. Dabei werden auch die angeforderten Sicherheits-Richtlinien, wie sie im SPD-Eintrag vorhanden sind, an das IKE-Modul übergeben. Eine IPSec-SA auszuhandeln wird als Phase-2-Verhandlung bezeichnet. Bevor jedoch eine IPSec-SA mit der Gegenstelle (Gateway) ausgehandelt werden kann, muss ein Kontrollkanal vom Client zum Gateway existieren. Dieser Kontrollkanal wird über die Phase-1-Verhandlung hergestellt, deren Ergebnis eine IKE-SA ist. Die Phase-1-Verhandlung übernimmt somit die komplette Authentisierung vom Client gegenüber dem VPN Gateway und erzeugt einen verschlüsselten Kontrollkanal. Über diesen Kontrollkanal kann dann rasch die Phase 2 (IPSec SA) durchgeführt werden. Die Phase-1-Verhandlung ist ein Handshake, über den auch der Austausch von Zertifikaten möglich ist und die den Schlüsselaustausch für den Kontrollkanal beinhaltet.

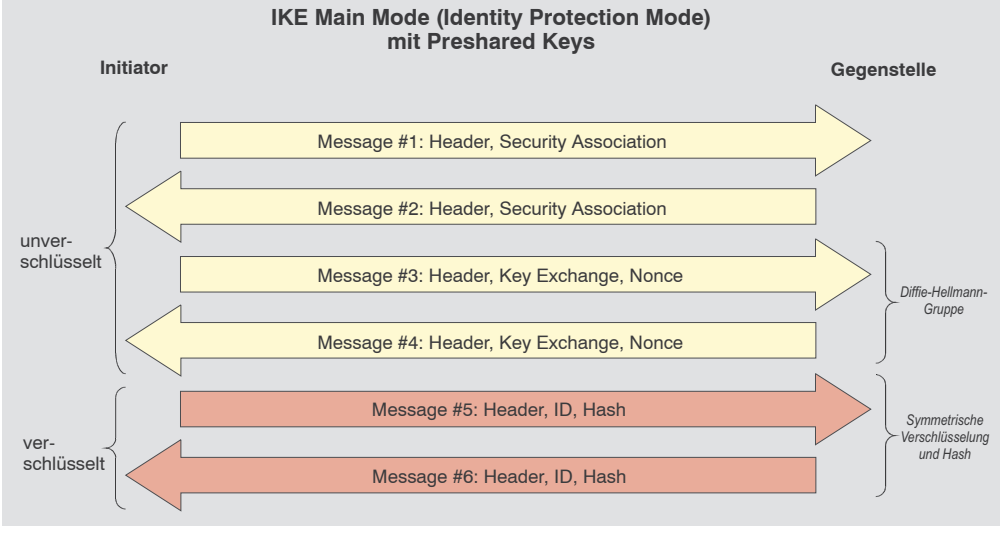
IKE-Modi

Im wesentlichen können zwei Arten der IKE-Richtlinien konfiguriert werden. Sie unterscheiden sich durch die Art der Authentisierung, entweder über Pre-shared Key oder über RSA-Signatur. Beide Arten des Internet Key Exchanges können in zwei unterschiedlichen Modi ausgeführt werden, dem Main Mode, auch Identity Protection Mode, oder dem Aggressive Mode. Die Modi unterscheiden sich durch die Anzahl der Messages und durch die Verschlüsselung.

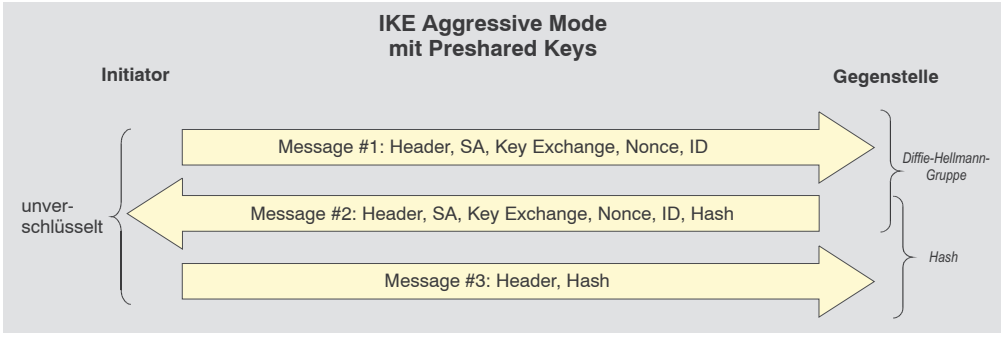
Im Main Mode (Standard-Einstellung) werden sechs Meldungen über den Kontrollkanal geschickt, wobei die beiden letzten, welche die User ID, das Zertifikat die Signatur und ggf. einen Hash-Wert beinhalten, verschlüsselt werden – daher auch Identity Protection Mode.

Im Aggressive Mode gehen nur drei Meldungen über den Kontrollkanal, wobei nichts verschlüsselt wird.

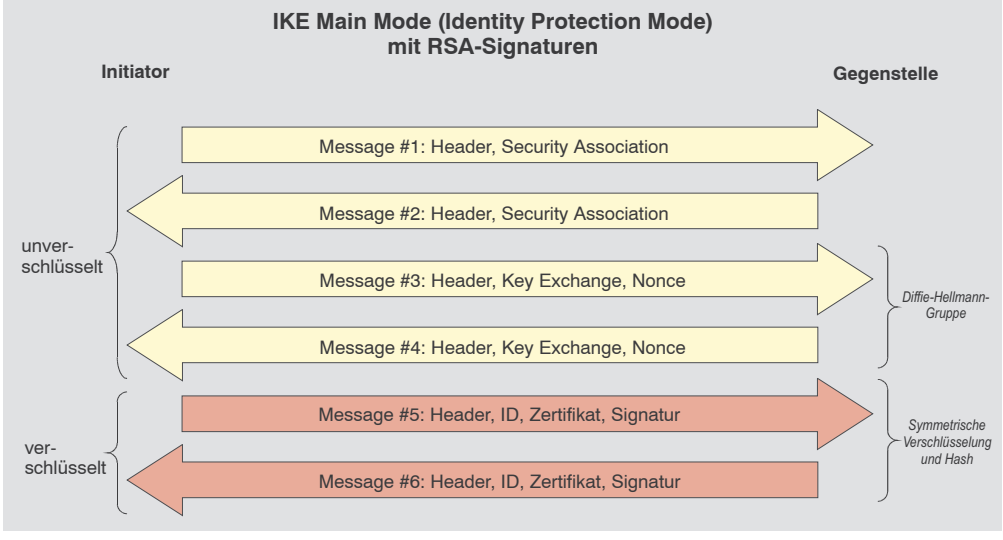
Den IKE-Modus (Austausch-Modus / Exchange Mode), Main Mode oder Aggressive Mode, bestimmen Sie in den Profil-Einstellungen im Parameterfeld “IPSec-Einstellungen”.



Wird die Pre-shared Key-Methode im Main Mode genutzt (Bild oben), so muss der Client am VPN/GW durch seine IP-Adresse eindeutig identifizierbar sein, da der Pre-shared Key mit in die symmetrische Schlüsselberechnung einbezogen und verschlüsselt wird, bevor sonstige Informationen übertragen werden, die den Client identifizieren könnten. Ein Client, der sich beim Provider einwählt, ist jedoch nicht durch die IP-Adresse zu erkennen, da er bei jeder Provider-Anwahl eine neue zugewiesen bekommt. Letztlich kann im Main Mode an alle Clients nur derselbe Pre-shared Key vergeben werden, was allerdings die Authentisierung abschwächt.



Eine Möglichkeit, einen allgmeinen Pre-shared Key zu vermeiden, wäre, den Aggressive Mode zu nutzen (Bild oben), doch wird dabei die ID des Clients nicht verschlüsselt.



Werden RSA-Signaturen eingesetzt (Bild oben und unten), so bedeutet dies, dass Zertfikate zum Einsatz kommen, womit die Vorkonfiguration jedweder "Secrets" überflüssig wird.

6.2.4 IPSec Tunneling

Der IPSec Client kann gegenüber IPSec-Gateways unterschiedlicher anderer Hersteller zum Einsatz kommen.

Die Kompatibilität mit den IPSec-Modi der anderen Hersteller beruht auf der Konformität mit folgenden RFCs und Drafts zu IPSec:

RFC 2104 - Keyed-Hashing for Message Authentication
RFC 2401 - Security Architecture for the Internet Protocol
RFC 2403 - The Use of HMAC-MD5-96 within ESP and AH
RFC 2404 - The Use of HMAC-SHA-1-96 within ESP and AH
RFC 2406 - IP Encapsulating Security Payload (ESP)
RFC 2407 - The Internet IP Security Domain of Interpretation for ISAKMP
RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2409 - The Internet Key Exchange (IKE)
DRAFT - draft-beaulieu-ike-xauth-05 (XAUTH)
DRAFT - draft-dukes-ike-mode-cfg-02 (IKECFG)
DRAFT - draft-ietf-ipsec-dpd-01 (DPD)
DRAFT - draft-ietf-ipsec-nat-t-ike-01 (NAT-T)
DRAFT - draft-ietf-ipsec-nat-t-ike-02 (NAT-T)
DRAFT - draft-ietf-ipsec-nat-t-ike-03 (NAT-T)
DRAFT - draft-ietf-ipsec-nat-t-ike-05 (NAT-T)
DRAFT - draft-ietf-ipsec-udp-encaps-06 (UDP-ENCAP)

■ **Implementierte Algorithmen für Phase 1 und 2:**

Unterstützte Authentisierung für Phase 1 (IKE-Richtlinie)

– RSA-Signatur

– PSK (Pre-shared Key)

Unterstützte symmetrische Verschlüsselungsalgorithmen (Phase 1 + 2)

– DES

– 3DES

– AES-128, AES-192, AES-256

Unterstützte asymmetrische Verschlüsselungsalgorithmen (Phase 1 + 2)

– DH 1,2,5 (Diffie-Hellmann)

– RSA

Unterstützte Hash-Algorithmen

– MD5

– SHA-1

Zusätzliche Unterstützung für Phase 2

– PFS (Perfect Forward Secrecy)

– IPCOMP (LZS)

– Seamless re-keying

In den Profil-Einstellungen des IPSec Clients werden automatisch einige Standards gesetzt:

– IKE Phase 1 Richtlinie - Automatischer Modus

– IKE Phase 2 Richtlinie - Automatischer Modus

– IKE Phase 1 Modus RSA - Main Mode

– IKE Phase 1 Modus PSK - Aggressive Mode

Diese automatisch gesetzten Richtlinien und Verhandlungsmodi sind in den Profil-Einstellungen konfigurierbar gehalten, sodass sie anderslautenden Verbindungsanforderungen entsprechend modifiziert werden können.

■ Standard IKE-Vorschläge:

1. Wenn für die IKE-Richtlinie der automatische Modus in den IPSec-Einstellungen gewählt wurde und im Parameterfeld “Identität” die Verwendung eines Pre-shared Keys nicht aktiviert wurde (ohne Haken!), so werden an die Gegenstelle standardmäßig folgende Vorschläge für die IKE-Richtlinie versendet, wobei die Authentisierung immer mit Zertifikat erfolgt:

Notation:

```
EA    = Encryption Algorithm (Verschlüsselung)
HASH  = Hash Algorithm (Hash)
AUTH  = Authentication Method (Authentisierung)
GROUP = Diffie-Hellmann Group Number (DH-Gruppe)
LT    = Life Type (Dauer)
LS    = Life Seconds (Dauer)
KL    = Key Length (Schlüssellänge)
```

EA	HASH	AUTH	GROUP	LT	LS	KL
AES_CBC	SHA	XAUTH_RSA	DH5	SECONDS	28800	256
AES_CBC	MD5	XAUTH_RSA	DH5	SECONDS	28800	256
AES_CBC	SHA	RSA	DH5	SECONDS	28800	256
AES_CBC	MD5	RSA	DH5	SECONDS	28800	256
AES_CBC	SHA	XAUTH_RSA	DH2	SECONDS	28800	256
AES_CBC	MD5	XAUTH_RSA	DH2	SECONDS	28800	256
AES_CBC	SHA	RSA	DH2	SECONDS	28800	256
AES_CBC	MD5	RSA	DH2	SECONDS	28800	256
AES_CBC	SHA	XAUTH_RSA	DH5	SECONDS	28800	192
AES_CBC	MD5	XAUTH_RSA	DH5	SECONDS	28800	192
AES_CBC	SHA	RSA	DH5	SECONDS	28800	192
AES_CBC	MD5	RSA	DH5	SECONDS	28800	192
AES_CBC	SHA	XAUTH_RSA	DH5	SECONDS	28800	128
AES_CBC	MD5	XAUTH_RSA	DH5	SECONDS	28800	128
AES_CBC	SHA	RSA	DH5	SECONDS	28800	128
AES_CBC	MD5	RSA	DH5	SECONDS	28800	128
AES_CBC	SHA	XAUTH_RSA	DH2	SECONDS	28800	128
AES_CBC	MD5	XAUTH_RSA	DH2	SECONDS	28800	128
AES_CBC	SHA	RSA	DH2	SECONDS	28800	128
AES_CBC	MD5	RSA	DH2	SECONDS	28800	128
DES3	SHA	XAUTH_RSA	DH5	SECONDS	28800	0
DES3	MD5	XAUTH_RSA	DH5	SECONDS	28800	0
DES3	SHA	RSA	DH5	SECONDS	28800	0
DES3	MD5	RSA	DH5	SECONDS	28800	0
DES3	SHA	XAUTH_RSA	DH2	SECONDS	28800	0
DES3	MD5	XAUTH_RSA	DH2	SECONDS	28800	0
DES3	SHA	RSA	DH2	SECONDS	28800	0
DES3	MD5	RSA	DH2	SECONDS	28800	0

Wird ein spezifischer IKE-Vorschlag in der IPSec-Konfiguration der Profil-Einstellungen eingestellt, so wird immer auch automatisch der gleiche Vorschlag zusätzlich mit Extended Authentication generiert und versendet.

2. Wird in das Feld für “Pre-shared Key” ein String eingetragen, so werden an die Gegenstelle standardmäßig folgende Vorschläge für die IKE-Richtlinie versendet, wobei die Authentisierung immer ohne Zertifikat erfolgt:

EA	HASH	AUTH	GROUP	LT	LS	KL
AES_CBC	SHA	XAUTH_PSK	DH5	SECONDS	28800	256
AES_CBC	MD5	XAUTH_PSK	DH5	SECONDS	28800	256
AES_CBC	SHA	PSK	DH5	SECONDS	28800	256
AES_CBC	MD5	PSK	DH5	SECONDS	28800	256
AES_CBC	SHA	XAUTH_PSK	DH2	SECONDS	28800	256
AES_CBC	MD5	XAUTH_PSK	DH2	SECONDS	28800	256
AES_CBC	SHA	PSK	DH2	SECONDS	28800	256
AES_CBC	MD5	PSK	DH2	SECONDS	28800	256
AES_CBC	SHA	XAUTH_PSK	DH5	SECONDS	28800	192
AES_CBC	MD5	XAUTH_PSK	DH5	SECONDS	28800	192
AES_CBC	SHA	PSK	DH5	SECONDS	28800	192
AES_CBC	MD5	PSK	DH5	SECONDS	28800	192
AES_CBC	SHA	XAUTH_PSK	DH5	SECONDS	28800	128
AES_CBC	MD5	XAUTH_PSK	DH5	SECONDS	28800	128
AES_CBC	SHA	PSK	DH5	SECONDS	28800	128
AES_CBC	MD5	PSK	DH5	SECONDS	28800	128
AES_CBC	SHA	XAUTH_PSK	DH2	SECONDS	28800	128
AES_CBC	MD5	XAUTH_PSK	DH2	SECONDS	28800	128
AES_CBC	SHA	PSK	DH2	SECONDS	28800	128
AES_CBC	MD5	PSK	DH2	SECONDS	28800	128
DES3	SHA	XAUTH_PSK	DH5	SECONDS	28800	0
DES3	MD5	XAUTH_PSK	DH5	SECONDS	28800	0
DES3	SHA	PSK	DH5	SECONDS	28800	0
DES3	MD5	PSK	DH5	SECONDS	28800	0
DES3	SHA	XAUTH_PSK	DH2	SECONDS	28800	0
DES3	MD5	XAUTH_PSK	DH2	SECONDS	28800	0
DES3	SHA	PSK	DH2	SECONDS	28800	0
DES3	MD5	PSK	DH2	SECONDS	28800	0

Als Vorschläge für die IPSec-Richtlinie (Phase 2) wird standardmäßig versendet:
Notation:

```
PROTO  - Protocol (Protokoll)
TRANS  - Transform (Transformation (ESP))
LT     - Life Type (Dauer)
LS     - Life Seconds (Dauer)
KL     - Key Length (Schlüssellänge)
COMP   - IP Compression (Transformation (Comp))
```

PROTO	TRANS	AUTH	LT	LS	KL	COMP	LZS
ESP	AES	MD5	SECONDS	28800	128	Yes	Yes
ESP	AES	SHA	SECONDS	28800	128	Yes	Yes
ESP	AES	MD5	SECONDS	28800	128	No	No
ESP	AES	SHA	SECONDS	28800	128	No	No
ESP	AES	MD5	SECONDS	28800	192	Yes	Yes
ESP	AES	SHA	SECONDS	28800	192	Yes	Yes
ESP	AES	MD5	SECONDS	28800	192	No	No
ESP	AES	SHA	SECONDS	28800	192	No	No
ESP	AES	MD5	SECONDS	28800	256	Yes	Yes
ESP	AES	SHA	SECONDS	28800	256	Yes	Yes
ESP	AES	MD5	SECONDS	28800	256	No	No
ESP	AES	SHA	SECONDS	28800	256	No	No
ESP	DES3	MD5	SECONDS	28800	0	Yes	Yes
ESP	DES3	MD5	SECONDS	28800	0	No	No

6.2.5 Zur weiteren Konfiguration

Pre-shared Key oder *RSA-Signatur*: Entsprechend den Vorgaben durch die Gegenstelle kann als “IKE-Richtlinie” die automatisch vorgenommene Einstellung “Automatischer Modus” auf “Pre-shared Key” oder “RSA Signatur” (Zertifikat) abgeändert werden. Erwartet die Gegenstelle “Pre-shared Key”, so muss der Schlüssel in das Feld eingetragen werden. (Der Pre-shared Key muss in diesem Fall für alle Clients identisch sein.)

IP-Adressen und *DNS Server* können über das Protokoll IKE-Config Mode (Draft 2) zugewiesen werden. Für die NAS-Einwahl können alle üblichen WAN-Schnittstellen verwendet werden.

Die *Authentisierung* bei IPSec Tunneling kann über das XAUTH Protokoll (Draft 6) erfolgen. Dazu müssen außerdem noch folgende Parameter im Konfigurationsfeld “Identität” gesetzt werden:

Benutzername	=	Kennwort des IPSec-Benutzers
Passwort	=	Passwort des IPSec-Benutzers
Zugangsdaten aus ...		
verwenden	=	optional

Bei IPSec Tunneling wird im Hintergrund automatisch DPD (Dead Peer Detection) und NAT-T (NAT Traversal) ausgeführt, falls dies von der Gegenstelle unterstützt wird. Mit DPD prüft der IPSec Client in bestimmten Abständen, ob die Gegenstelle noch aktiv ist. Bei inaktiver Gegenstelle erfolgt ein automatischer Verbindungsabbau. Unterstützt die Gegenstelle DPD nicht, so kann DPD im Parameterfeld “IPSec-Einstellungen” deaktiviert werden. Der Einsatz von NAT Traversal erfolgt beim IPSec Client automatisch und ist immer nötig, wenn auf dem weg zum Zielsystem ein Gerät mit Network Address Translation zum Einsatz kommt.

■ Basiskonfigurationen in Abhängigkeit vom IPSec Gateway

Im folgenden sind Konfigurationsmöglichkeiten aufgeführt, die zu beachten sind, je nachdem ob das IPSec Gateway Extended Authentication (XAUTH) und IKE-Config Mode unterstützt oder nicht.

Gateway unterstützt nicht XAUTH

Der IPSec Client als Initiator der IPSec-Verbindung schlägt standardmäßig immer die Extended Authentication vor. Diese Eigenschaft kann nicht konfiguriert werden. Unterstützt das Gateway die Extended Authentication nicht, so wird sie auch nicht durchgeführt.

Gateway unterstützt IKE-Config Mode

Sofern das Gateway den IKE-Config Mode unterstützt, kann im Parameterfeld “IP-Adressen-Zuweisung” die Funktion “IKE Config Mode verwenden" aktiviert werden.

Gateway unterstützt IKE-Config Mode nicht

Unterstützt das Gateway den IKE-Config Mode nicht, so sind zwei Konfigurationen möglich.

1. Wird die Funktion “IP-Adresse manuell vergeben” (siehe → Profil-Einstellungen, IP-Adressen-Zuweisung) aktiviert, so muss die IP-Adresse eingetragen werden, die vom Gateway bzw. Administrator für diesen Client bzw. Benutzer vorgegeben wurde.

2. Wird “Lokale IP-Adresse verwenden” (siehe → Profil-Einstellungen, IP-Adressen-Zuweisung) aktiviert, so wird die IP-Adresse gleich der öffentlichen IP-Adresse gesetzt, die der Client pro Internet Session vom Provider erhält oder, unter der Verbindungsart “LAN”, die Adresse, die der LAN-Adapter besitzt.

   Wird die lokale IP-Adresse verwendet und der “Typ” im Parameterfeld “Identität” steht auf “IP-Adresse”, dann darf im Feld für die “ID” keine IP-Adresse eingetragen sein. Nur dann ist gewährleistet, dass die jeweils aktuelle öffentliche IP-Adresse automatisch zur Identifikation für Phase 1 an das Gateway übertragen wird.

6.2.6 IPSec Ports für Verbindungsaufbau und Datenverkehr

Bitte beachten Sie, dass der IPSec Client exklusiven Zugriff auf den UDP Port 500 benötigt. Sofern NAT Traversal eingesetzt wird, wird auch Zugriff auf Port 4500 benötigt. Ohne NAT Traversal wird das IP-Protokoll ESP (Protokoll-ID 50) benutzt.

Standardmäßig wird der Port 500, der für den Verbindungsaufbau genutzt wird, unter Windows-Systemen von den IPSec-Richtlinien genutzt. Um dies zu ändern gehen Sie wie folgt vor:

1. Um sich zu vergewissern, welche Ports aktuell von Ihrem System genutzt werden, können Sie unter der MS-DOS-Eingabeaufforderung mit dem Kommando

   `netstat -n -a`

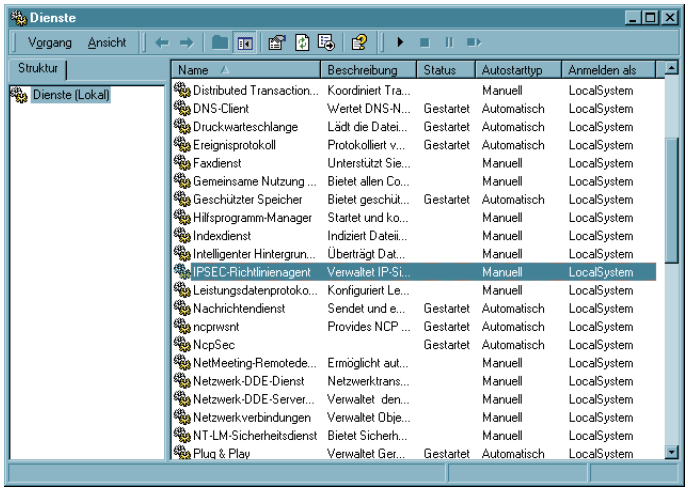
   den aktuellen Netzstatus anzeigen lassen. In der Abbildung rechts erkennen Sie, dass der UDP Port 500 genutzt wird.

```
F:\>netstat -n -a

Aktive Verbindungen

  Proto  Lokale Adresse          Remoteadresse        Status
  TCP    0.0.0.0:135             0.0.0.0:0            ABHöREN
  TCP    0.0.0.0:445             0.0.0.0:0            ABHöREN
  TCP    0.0.0.0:1025            0.0.0.0:0            ABHöREN
  TCP    0.0.0.0:1032            0.0.0.0:0            ABHöREN
  TCP    0.0.0.0:5000            0.0.0.0:0            ABHöREN
  TCP    172.16.113.140:139      0.0.0.0:0            ABHöREN
  TCP    172.16.113.140:1032     62.153.165.34:21     HERGESTELLT
  UDP    0.0.0.0:135             *:*
  UDP    0.0.0.0:162             *:*
  UDP    0.0.0.0:445             *:*
  UDP    0.0.0.0:500             *:*
  UDP    0.0.0.0:1027            *:*
  UDP    0.0.0.0:1028            *:*
  UDP    127.0.0.1:123           *:*
  UDP    127.0.0.1:1900          *:*
  UDP    172.16.113.140:123      *:*
  UDP    172.16.113.140:137      *:*
  UDP    172.16.113.140:138      *:*
  UDP    172.16.113.140:1900     *:*
```

2. Wird der Port genutzt, so muss im Windows-Startmenü das Fenster “Sytem → Dienste-Verwaltung” geöffnet werden. Dort wird der “IPSEC-Richtlinienagent” markiert, der Dienst gestoppt und der “Autostarttyp” auf “Manuell” gestellt (Bild rechts).



3. Wurde die Änderung des Autostarttyps durchgeführt, so kann das Kommando

   `netstat -n -a`

   erneut ausgeführt werden. Der UDP Port 500 darf dann unter den aktiven Verbindungen nicht mehr aufgeführt sein.

6.3 Zertifikats-Überprüfungen

Neben der Zertifikats-Überprüfung nach Inhalten erfolgt am IPSec Client eine weitere Zertifikatsprüfung in mehrfacher Hinsicht.

6.3.1. Auswahl der CA-Zertifikate

Der Administrator des Firmennetzes legt fest, welchen Ausstellern von Zertifikaten vertraut werden kann. Dies geschieht dadurch, dass er die CA-Zertifikate seiner Wahl in das Windows-Verzeichnis \ncple\cacerts\ gespielt. Das Einspielen kann bei einer Software-Distribution mit Disketten automatisiert stattfinden, wenn sich die Aussteller-Zertifikate bei der Installation der Software im Root-Verzeichnis der ersten Diskette befinden (siehe → CA-Zertifikate anzeigen).

Derzeit werden die Formate *.pem und *.crt für Aussteller-Zertifikate unterstützt. Sie können im Monitor unter dem Hauptmenüpunkt “Verbindung – Zertifikate – CA-Zertifikate anzeigen” eingesehen werden.

Wird am IPSec Client das Zertifikat einer Gegenstelle empfangen, so ermittelt der NCP Client den Aussteller und sucht anschließend das Aussteller-Zertifikat, zunächst auf Smart Card oder PKCS#12-Datei, anschließend im Verzeichnis NCPLE\CACERTS\. Kann das Aussteller-Zertifikat nicht gefunden werden, kommt die Verbindung nicht zustande. Sind keine Aussteller-Zertifikate vorhanden, wird keine Verbindung zugelassen.

6.3.2. Überprüfung der Zertifikats-Erweiterung

Zertifikate können Erweiterungen (Extensions) erfahren. Diese dienen zur Verknüpfung von zusätzlichen Attributen mit Benutzern oder öffentlichen Schlüsseln, die für die Verwaltung und den Betrieb der Zerifizierungshierarchie und der Sperrlisten (Revocation Lists) benötigt werden. Prinzipiell können Zertifikate eine beliebige Anzahl von Erweiterungen inklusive privat definierter beinhalten. Die Zertifikats-Erweiterungen (Extensions) werden von der ausstellenden Certification Authority in das Zertifikat geschrieben. Für den IPSec Client und das Gateway sind drei Erweiterungen von Bedeutung:

- ☐ extendedKeyUsage
- ☐ subjectKeyIdentifier
- ☐ authorityKeyIdentifier

- **extendedKeyUsage**

  Befindet sich in einem eingehenden Benutzer-Zertifikat die Erweiterung extendedKeyUsage so prüft der IPSec Client, ob der definierte erweiterte Verwendungszweck “SSL-Server-Authentisierung” enthalten ist. Ist das eingehende Zertifikat nicht zur Server-Authentisierung vorgesehen, so wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

  Bitte beachten Sie, dass die SSL-Server-Authentisierung richtungsabhängig ist. D.h. der Initiator des Tunnelaufbaus prüft das eingehende Zertifikat der Gegenstelle, das, sofern die Erweiterung extendedKeyUsage vorhanden ist, den Verwendungszweck “SSL-Server-Authentisierung” beinhalten muss. Dies gilt auch bei einem Rückruf an den Client über VPN.

  Ausnahme: Bei einem Rückruf des Servers an den Client nach einer Direkteinwahl ohne VPN aber mit PKI prüft der Server das Zertifikat des Clients auf die Erweiterung extendedKeyUsage. Ist diese vorhanden, muss der Verwendungszweck “SSL-Server-Authentisierung” beinhaltet sein, sonst wird die Verbindung abgelehnt. Ist diese Erweiterung nicht im Zertifikat vorhanden, so wird diese ignoriert.

- **subjectKeyIdentifier / authorityKeyIdentifier**

  Ein keyIdentifier ist eine zusätzliche ID (Hashwert) zum CA-Namen auf einem Zertifikat. Der authorityKeyIdentifier (SHA1-Hash über den public Key des Ausstellers) am eingehenden Zertifikat muss mit dem subjectKeyIdentifier (SHA1-Hash über den public Key des Inhabers) am entsprechenden CA-Zertifikat übereinstimmen. Kann keine Übereinstimmung erkannt werden, wird die Verbindung abgelehnt.

  Der keyIdentifier kennzeichnet den öffentlichen Schlüssel der Zertifizierungsstelle und somit nicht nur eine, sondern gegebenenfalls eine Reihe von Zertifikaten. Damit erlaubt die Verwendung des keyIdentifiers eine größere Flexibilität zum Auffinden eines Zertifizierungspfades.

  (Außerdem müssen die Zertifikate, die den keyIdentifier in der authorityKeyIdentifier-Erweiterung besitzen, nicht zurückgezogen werden, wenn die CA sich bei gleichbleibendem Schlüssel ein neues Zertifikat ausstellen lässt.)

6.3.3. Überprüfung von Sperrlisten

Zu jedem Aussteller-Zertifikat kann dem IPSec Client die zugehörige CRL (Certificate Revocation List) zur Verfügung gestellt werden. Sie wird in das Windows-Verzeichnis \ncple\crls\ gespielt. Ist eine CRL vorhanden, so überprüft der IPSec Client eingehende Zertifikate daraufhin, ob sie in der CRL geführt sind. Gleiches gilt für eine ARL (Authority Revocation List), die in das Windows-Verzeichnis \ncple\arls\ gespielt werden muss.

6.4 Stateful Inspection-Technologie für die Firewall-Einstellungen

Die Firewall-Technologie der Stateful Inspection kann für alle Netzwerkadapter wie auch für RAS-Verbindungen eingesetzt werden. Sie wird am Client im Telefonbuch unter “Firewall-Einstellungen” aktiviert (siehe → Konfigurations-Parameter, Firewall-Einstellungen). Am Gateway ist sie dann aktiv, wenn im Server Manager unter “Routing Interfaces – Allgemein” die Funktion “LAN-Adapter schützen” eingeschaltet wird.

Grundsätzliche Aufgabe einer Firewall ist es, zu verhindern, dass sich Gefahren aus anderen bzw. externen Netzen (Internet) in das eigene Netzwerk ausbreiten. Deshalb wird eine Firewall auch am Übergang zwischen Firmennetz und z.B. Internet installiert. Sie prüft alle ein- und ausgehenden Datenpakete und entscheidet auf der Basis vorher festgelegter Konfigurationen, ab ein Datenpaket durchgelassen wird oder nicht.

Stateful Inspection ist die Firewall-Technologie, die den derzeit höchstmöglichen Sicherheitsstandard für Internet-Verbindungen und somit das Firmennetz bietet. Sicherheit wird in zweierlei Hinsicht gewährleistet. Zum einen verhindert diese Funktionalität den unbefugten Zugriff auf Daten und Ressourcen im zentralen Datennetz. Zum anderen überwacht sie als Kontrollinstanz den jeweiligen Status aller bestehenden Internet-Verbindungen. Die Stateful Inspection Firewall erkennt darüber hinaus, ob eine Verbindung “Tochterverbindungen” geöffnet hat – wie beispielsweise bei FTP oder Netmeeting – deren Pakete ebenfalls weitergeleitet werden müssen. Für die Kommunikationspartner stellt sich eine Stateful Inspection-Verbindung als eine direkte Leitung dar, die nur für einen den vereinbarten Regeln entsprechenden Datenaustausch genutzt werden darf. Alternative Bezeichnungen für Stateful Inspection sind: Stateful Packet Filter, Dynamic Packet Filter, Smart Filtering, Adaptive Screening.

Stateful Inspection vereinigt konzeptionell die Schutzmöglichkeiten von Packet Filter und Application Level Gateways d.h. sie integriert als Hybrid die Funktionen beider Security-Verfahren und arbeitet sowohl auf der Netz- als auch Anwenderschicht. Bei der “zustandsabhängigen Paket-Filterung” werden nicht nur die Internet- und Transportschicht sondern auch Abhängigkeiten vom Zustand einer Verbindung berücksichtigt. Alle aktuellen und initiierten Verbindungen werden mit Adresse und zugeordnetem Port in einer dynamischen Verbindungstabelle hinterlegt. Der Stateful Inspection-Filter entscheidet anhand festgelegter Raster (Informationen), welche Pakete zu welcher Verbindung gehören. Zustände können sein: Verbindungsaufbau, Übertragung, Verbindungsabbau und gelten sowohl für TCP- als auch UDP-Verbindungen. Ein Beispiel an einer Telnet-Sitzung: Der Zustand “Verbindungsaufbau” wird dadurch definiert, dass noch keine Benutzer-Authentisierung stattgefunden hat. Hat der Benutzer sich mit Benutzername und Kennwort angemeldet, wird diese Verbindung in den Zustand “normale Verbindung” gesetzt. Da der jeweilige Status einer Verbindung ständig überwacht wird, bleibt Unbefugten der Zugriff auf das interne Unternehmensnetz verwehrt.

Der Vorteil gegenüber statischen Paketfiltern ist, dass die Entscheidung, ob ein NCP Secure Gateway oder Client ein Paket weiterleitet oder nicht, nicht nur auf Grund von Quell- und Zieladresse oder Ports fällt. Das Security-Management prüft darüber hinaus

den Zustand (state) der Verbindung zu einem Partner. Weitergeleitet werden ausschließlich die Pakete, die zu einer aktiven Verbindung gehören. Datenpakete, die sich keiner etablierten Verbindung zuordnen lassen, werden verworfen und im Log-File protokolliert. Neue Verbindungen lassen sich nur entsprechend der konfigurierten Regeln öffnen.

In der einfachsten Firewall-Funktion werden nur die ein- und ausgehenden Verbindungen im Hinblick auf das Protokoll (TCP/IP, UDP/IP, ICMP, IPX/SPX), die entsprechenden Ports und die beteiligten Rechner überprüft und überwacht. Verbindungen werden in Abhängigkeit eines festgelegten Regelwerkes erlaubt oder gesperrt. Weitere Prüfungen (z.B. Inhalt der übertragenen Daten) finden nicht statt.

Die Stateful Inspection Filter sind eine Weiterentwicklung der dynamischen Packet-Filter und bieten eine komplexere Logik. Die Firewall prüft, ob eine am Portfilter erlaubte Verbindung auch zu dem definierten Zweck aufgebaut wird.

Es werden folgende zusätzliche Informationen zu einer Verbindung verwaltet:

– Nr. zur Identifizierung einer Verbindung
– Zustand der Verbindung (z.B. Aufbau, Datenübertragung, Abbau)
– Quell-Adresse des ersten Pakets
– Ziel-Adresse des ersten Pakets
– Interface, durch welches das erste Paket kam
– Interface, durch welches das erste Paket verschickt wurde

Anhand dieser Informationen kann der Filter entscheiden, welche nachfolgenden Pakete zu welcher Verbindung gehören. So kann ein Stateful Inspection-System auch das UDP-Problem ausschalten. Hintergrund ist die verhältnismäßig leichte Fälschbarkeit von UDP-Paketen z.B. beim UDP-basierten Dienst DNS. Da Stateful Inspection-Filter in der Lage sind, sich die aktuelle Status- und Kontextinformation einer Kommunikationsbeziehung zu merken, ist es erforderlich, dass neben der Quell- und Zieladresse sowie Quell- und Zielport, auch der DNS-Header im Anfrage-Paket in die Speicherung der Status- und Kontextinformation einbezogen wird. Es erfolgt eine Interpretation auf der Anwendungsschicht.

Beispiel: Eine gehenden Verbindung zum Port 21 eines Rechners ist für einen reinen Portfilter eine FTP-Verbindung. Eine weitere Überprüfung findet nicht statt. Der Stateful Inspection-Filter prüft zusätzlich, ob die über diese Verbindung übertragenen Daten zu einer etablierten FTP-Verbindung gehören. Wenn nicht, wird die Verbindung sofort unterbrochen. Weiter ist ein Stateful Inspection-Filter in der Lage, Regeln in Abhängigkeit von notwendigen Kommunikationsprozessen anzupassen. Wenn z.B. eine abgehende FTP-Verbindung erlaubt ist, so ermöglicht die Firewall auch automatisch die Etablierung des zugehörigen Rückkanals. Die entsprechenden Informationen (Ports) werden aus der Kontrollverbindung herausgelesen.

Ein vorteilhafter Aspekt von Stateful Inspection-Filtern ist die Fähigkeit, die Daten auf allen Protokollebenen (d.h. von Netzwerk- bis Anwendungsebene) zu prüfen. So kann z.B. ein FTP-GET erlaubt, ein FTP-PUT jedoch verboten werden. Ein positiver Effekt der im Vergleich zu konventionellen Paketfiltern erhöhten Eigenintelligenz ist die Opti-

on, einzelne Pakete während einer Kommunikationsbeziehung zu assemblieren und damit erweiterte Möglichkeiten zur Benutzer-Authentisierung zur Anwendung zu bringen. Als Folge der nicht verlässlichen Trennung der Netzwerksegmente sind Stateful Inspection-Filter nicht immun gegen bestimmte auf unteren Protokollebenen stattfindende Angriffe. So z.B. werden fragmentierte Pakete i.d.R. von außen nach innen ohne weitere Prüfung durchgelassen.

Abkürzungen und Begriffe

3DES	TripleDES. Verschlüsselungsstandard mit 112 Bit.
AES	Advanced Encryption Standard. Europäische Entwicklung der belgischen Verschlüsselungsexperten Joan Daemen und Vincent Rijmen (“Rijndael-Algorithmus”). Nachfolger von DES (Data Encryption Standard). Verschlüsselungsalgorithmus, der bis zu 256 Bit Schlüssellänge besitzt. n hoch 256 gilt als Maßeinheit für die mögliche Anzahl der Schlüssel, die mit diesem Algorithmus generiert werden können. Trotz steigender Prozessorgeschwindigkeiten wird erwartet, dass der AES-Algorithmus eine akzeptable Sicherheit für die nächsten 30 Jahre bietet. Wird in VPN- und SSL-Verschlüsselungen bald große Verbreitung finden.
AH	Authentication Header RFC 2402
Asymmetrische Verschlüsselung	(Public-Key-Verfahren) Bei einer asymmetrischen Verschlüsselung besitzt jeder Teilnehmer zwei Schlüssel: einen geheimen, privaten und einen öffentlichen Schlüssel. Beide Schlüssel stehen in einer mathematisch definierten Beziehung zueinander. Der private Schlüssel des Teilnehmer ist streng geheim, der öffentliche Schlüssel für jedermann zugänglich. Das Schlüsselmanagement gestaltet sich auch bei großen Teilnehmerzahlen überschaubar: Zwei Schlüssel pro Teilnehmer – ergibt insgesamt 2.000 Schlüssel, um 1.000 Teilnehmern in allen Sender-Empfänger-Kombinationen die sichere Kommunikation zu ermöglichen. Das bekannteste asymmetrische Verschlüsselungsverfahren ist RSA. Nachteil der asymmetrischen Verfahren: Sie sind rechenintensiv und damit vergleichsweise langsam.

Basisanschluss (So / BRI = Basic Rate Interface)	ISDN-Anschlusstyp mit So-Schnittstelle (“S” für Subscriber Interface: Benutzerschnittstelle), bestehend aus einem D-Kanal (Bandbreite: 16 kBit/s) für die Steuerung und zwei B-Kanälen (Bandbreite jeweils 64 kBit/s) für die Übertragung von Nutzinformationen.
BCP	Bridge Control Protocol
BITS	Bump In The Stack. Art der Implementierung von IPsec.
BITW	Bump In The Wire. Art der Implementierung von IPsec.
Blowfish	Verschlüsselungsstandard mit 128/448 Bit
BRI	Basic Rate Interface (ISDN-Schnittstelle, Basis So) mit 2 B-Kanälen und 1 D-Kanal.
Browser	Der Browser stellt die Anwender-Schnittstelle zum Internet dar. Mit seiner HTTP-Fähigkeit (Hypertext-Transfer-Protokoll) kann er verschiedene Formate (z.B. HTML, GIF, CAD), die für eine multimediale Darstellung der Information benötigt werden, in Sound und Grafik umsetzen.
CA	Certification Authority, auch Trust Center (z.B. D-Trust, ein Gemeinschaftsunternehmen der Bundesdruckerei und Debis). Eine CA stellt mittels PKI-Manager (Software) digital signierte Bestätigungen (Zertifikate) aus und brennt sie auf eine Smartcard (Chipkarte). Eine CA kann ein privater Dienstleister oder eine öffentiche Einrichtung sein. Diese Zertifizierungsstellen bedürfen nicht der Genehmigung durch den Staat. Sie haften für die Richtigkeit der Zertifikate.
CAPI	Common Application Programm Interface. Diese Schnittstelle wird im ISDN als Common ISDN API bezeichnet und entspricht der PCI-Schnittstelle (Programmable Communication Interface). Die Schnittstelle erlaubt den direkten Zugang zum ISDN und den unteren Protokoll-schichten (Ebene 1-3). Höhere Protokolle (Anwendungen) wie Telex oder Filetransfer können unabhängig von der eingesetzten Hardware-Plattform verwendet werden. Die CAPI gibt es in zwei Versionen, 1.1 und 2.0.

	Entsprechend sind auch dieISDN-Anwendungsprogramme programmiert, die entweder auf CAPI 1.1 oder CAPI 2.0 aufsetzen, bzw. die jeweilige CAPI voraussetzen. Eine Hybrid-CAPI gestattet sowohl den Einsatz einer Anwendungs-Software für CAPI 1.1 als auch den von CAPI 2.0-Software. (Siehe Hybrid-CAPI)
CCP	Compression Control Protocol
CHAP	Challenge Handshake Authentication Protocol
CLI	Calling Line Identification (Rufnummern-Identifizierung im Euro-ISDN)
COSO	Charge One Side Only. COSO-Rückruf, auch Low Level- oder D-Kanal Rückruf. Für den Initiator des Rückrufs im D-Kanal fallen keine Gebühren an.
CTAPI	Schnittstelle zu Smartcard Readern
CUG	Closed User Group (geschlossene Benutzergruppe im Euro-ISDN)
DES	Datenverschlüsselungsnorm, Data Encryption Standard
DHCP	Mit DHCP (Dynamic Host Control Protocol) zu kommunizieren, bedeutet, dass für jede Session automatisch eine IP-Adresse zugewiesen wird.
Directory Service	Remote Access-Zugänge werden wie E-Mail-Adressen, Telefonnummern etc. in Verzeichnissen auf unterschiedlichen Datenbanken abgelegt. Das Problem bei dieser Vielzahl von Verzeichnissen ist, dass einerseits viele Daten mehrfach erfasst werden und zudem die einzelnen Einträge nicht untereinander verknüpft sind. Der Pflegeaufwand ist enorm und Inkonsistenzen sind nicht auszuschließen. Gefordert ist ein standardisiertes Prozedere, mit Hilfe dessen die Erfassung und Pflege aller Informationen in einer zentralen Directory ermöglicht wird. Das T-Online Security Management unterstützt die standardisierten Protokolle Radius (Remote Authorization Dial In User Service) und LDAP (Lightweight Directory Access Protocol), wobei letztere den Zugriff auf zentralisierte Verzeichnisdienste gewährleistet.

DMZ	Demilitarisierte Zone, zwischen Firewall und Unternehmensnetz, zum Beispiel mit Web-, Email- und VPN-Server.
DNS	Der Domain Name Server (DNS) stellt die IP-Adresse für eine Internet-Sitzung zur Verfügung, nachdem die Anwahl mit Benutzername und Passwort erfolgte. Er routet weiter im Internet, indem er die Namen, die im Browser als gewünschtes Ziel angegeben werden, in IP-Adressen rückübersetzt und die Verbindung zu dieser Adresse herstellt.
D-Kanal-Protokoll	Das D-Kanal-Protokoll sorgt dafür, dass sich Endgeräte mit dem Netz verständigen können. Es steuert unter anderem Verbindungsauf- und abbau. Es umfasst Schicht 2 und 3. Auf Schicht 2 von ISDN ist HDLC für die logische Datenübertragungssteuerung eingesetzt. Das eigentliche D-Kanal-Protokoll ist auf Schicht 3 angesiedelt. Mittlerweile ist DSS1 als europaweites D-Kanal-Protokoll verfügbar.
DSA	Directory System Agent
DSS1	European Digital Subscriber System No. 1. Europäisches ISDN-Protokoll für den D-Kanal.
DUA	Directory User Agent
ECP	Encryption Control Protocol
ESP	Encapsulating Security Payload RFC 2406
Euro-ISDN	ITU-Standard für Europäisches ISDN; bezieht sich auf das D-Kanal-Protokoll DSS1 und mögliche Dienstmerkmale, wie Gebührenanzeige (Advice of Charge), Rückruf bei Besetzt (Completion of Calls to Busy Subscriber), Rufumleitung (Call Forwarding), Anklopfen (Call Waiting), etc. Im Euro-ISDN mit dem D-Kanal-Protokoll DSS1 werden einzelne Endgeräte mit der Multible Subscriber Number (MSN) adressiert.
Firewall	Trennt Public-Netz von Private-Netz. Schutzmechanismus in Netzen, der den Zugriff der Stationen regelt. Ein Firewall-Rechner schottet ein Netzwerk

vor allem WAN-seitig gegen unautorisierten Zugriff ab. Die Berechtigung kommender und abgehender Verbindungen wird zum Beispiel geregelt durch Herausfiltern bestimmter Netzteilnehmer und Netzdienste und Festlegung der Zugriffsberechtigungen. Vom WAN aus betrachtet stehen hinter der Firewall (in der DMZ) für gewöhnlich Web-Server, Email-Server und VPN-Server.

FTP File Transfer Protocol. Basiert auf TCP und dem Terminalprotokoll TELNET (Port 21).

GPRS Standard für schnelle Handy-Kommunikation

GRE Generic Router Encapsulation. CISO-Spezifisches Tunnel-Protokoll.

GSM Global System Mobile. Standard für Handy-Kommunikation

Hash-Wert siehe Signatur

HBCI Standard für Smartcard Reader (Online Banking)

HTTP Hypertext Transfer Protocol. Multimedia-Network im Internet (Port 80)

Hybride Verschlüsselung Hohe Performance plus viel Sicherheit: Hybride Verschlüsselung vereint die Vorteile symmetrischer und asymmetrischer Verfahren. Während die Inhalte der Kommunikation mit schnellen symmetrischen Algorithmen gesichert werden, erfolgen Authentisierung der Teilnehmer und Schlüsselaustausch auf Basis asymmetrischer Verfahren. Die eigentliche Verschlüsselung der Daten eines Dokuments geschieht auf Basis einer Zufallszahl (Session-Key), die für jede einzelne Kommunikationsverbindung neu erzeugt wird. Dieser Einmalschlüssel wird mit dem öffentlichen Schlüssel des Empfängers chiffriert und der Nachricht beigefügt. Der Empfänger wiederum rekonstruiert mit seinem privaten Schlüssel den Session-Key und entschlüsselt die Nachricht.

IETF Internet Engineering Task Force. Interessengemeinschaft, die sich mit Problemen des TCP/IP und dem Internet befasst, unter anderem den Well Known Ports (Ports 0 bis 1023).

IKE

Internet Key Exchange. Bestandteil von IPsec für sicheres Schlüssel-Management. Separate security association negotiation and key management protocol RFC 2409

Internet

Das Internet ist ein weltweites, offenes Rechnernetz. Es ist allgemein zugänglich. Jeder Betrieb und jede Privatperson kann sich daran anschließen und mit allen anderen angeschlossenen Benutzern kommunizieren, unabhängig von der eingesetzten Rechnerplattform oder der jeweiligen Netztopologie. Damit der Datenaustausch zwischen den unterschiedlichen Rechnern und Netzen innerhalb des Internets möglich wird, ist ein allen gemeinsames Netzwerkprotokoll nötig. (siehe TCP/IP)

IP-Adresse

Jeder Rechner im Internet besitzt für die Dauer seiner Zugehörigkeit zum Internet eine IP-Adresse (Internet-Protokoll-Adresse), die ihn eindeutig identifiziert. Eine IP-Adresse ist 32 Bits lang und besteht aus vier voneinander durch Punkte getrennte Zahlen. Für jede Zahl stehen 8 Bits zur Verfügung, womit sie 256 Werte annehmen kann. Die Anzahl der möglichen IP-Adressen insgesamt bleibt jedoch begrenzt. Der Internet-User bekommt daher nicht einmalig eine unveränderliche IP-Adresse zugeteilt, sondern für jede seiner Sessions die IP-Adresse, die gerade noch nicht vergeben ist. Die IP-Adressen werden also für die Dauer eines Zeitschlitzes zugeteilt. Diese Adress-Zuteilung erfolgt im Regelfall automatisch per PPP-Verhandlung über DHCP. Die IP-Adresse kann von speziellen Programmen in einen Namen übersetzt werden. Diese Programme laufen auf einem Domain Name Server (DNS).

IP Network Address Translation

(IP Network Address Translation wird bei der Installation der Workstation Software bereits vorgesehen und ist standardmäßig beim Anlegen eines neues Zielsystems aktiviert!) Wenn IP Network Address Translation verwendet wird, werden alle übertragenen Frames mit der ausgehandelten (PPP) IP-Adresse verschickt. Die Workstation Software übersetzt diese öffentliche IP-Adresse in die systemeigene des Intranets oder, im Falle der Workstation, in deren eigene vom Benutzer festgelegte. Allgemein: Über NAT ist es möglich, in einem LAN mit inoffiziellen IP-Adressen, die nicht im

	Internet gültig sind, zu arbeiten und trotzdem vom LAN aus auf das Internet zuzugreifen. Dazu werden die inoffiziellen IP-Adressen von der Software in offizielle IP-Adressen übersetzt. Dies spart zum einen ofizielle IP-Adressen, die nicht in unbegrenzter Anzahl zur Verfügung stehen. Zum anderen wird damit ein gewisser Schutz (Firewall) für das LAN aufgebaut.
IPCP	Internet Protocol Control Protocol
IPsec	Standards festgelegt von IETF: RFCs 2401-2412 (12/98)
IPX	Internet Packet Exchange, Netware-Protokoll von Novell
IPXCP	Internetwork Packet Exchange Control Protocol
ISDN	Integrated Services Digital Network. Dienste-integrierendes digitales Fernmeldenetz. Digitales Netz mit Integration aller Schmalband-Kommunikationsdienste (z.B. Fernsprechen, Telex, Telefax, Teletext, Bildschirmtext), bestehend aus Kanälen mit einer Übertragungsgeschwindigkeit von 64.000 bit/s. Ein Basisanschluss im sogenannten Schmalband-ISDN besitzt drei Übertragungskanäle:Kanal B1: 64.000 bit/sKanal B2: 64.000 bit/sKanal D: 16.000 bit/sDie Gesamtübertragungsrate beträgt 144.000 bit/s. Dieses Netz soll bis zum Ende dieses Jahrtausends europaweit einheitlich aufgebaut werden. Die Spezifikationen hierfür werden von ITU und CEPT erarbeitet.
ISDN-Adapter	ISDN-Adapter ermöglichen den Anschluss von vorhandenen, nicht ISDN-fähigen Endgeräten an das ISDN. Der Adapter übernimmt dabei die sowohl soft- als auch hardwaremäßige Anpassung der Endgeräteschnittstelle an die ISDN-Schnittstelle (So). Ein ISDN-Adapter mit Upo-Schnittstelle ermöglicht an ISDN TK-Anlagen die Umsetzung der ISDN-Zweidraht-Schnittstelle Upo (Reichweite ca. 3,5km) auf die busfähige ISDN-Vierdraht-Schnittstelle So (Reichweite ca. 150m) nach den Richtlinien der Telekom.
ISP	Internet Service Provider

Kryptographie	Anwendungen sind Verschlüsselung, elektronische Signatur, Authentifikation und Hash-Wert-Berechnung. Mathematische Verfahren, die mit Schlüssel verwendet werden.
LCP	Link Control Protocol
LDAP	Lightweight Directory Access Protocol, siehe Directory Service
MAC-Adresse	Medium Access Control Layer-Adresse. Physikalische Adresse im Netzwerk.
MIB	Management Information Base. Beschreibt die Struktur der Managementinformationen beim SNMP.
MD5	Message Digit 5. Verfahren zur Bildung eines Hash-Werts
NAS	Network Access System
NetBios	Network Basic Input Output System. Schnittstelle, die Datagramm- und streamorientierte Kommunikation bietet.
OCSP	Online Certificate Status Protocol. Wird als Protokoll für die Online-Prüfung von Zertifikaten verwendet.
OSI-Referenzmodell	Von der ISO standardisiertes Modell, das Kommunikation in sieben Schichten beschreibt: 7. Anwendungsschicht (application layer), 6. Darstellungsschicht (presentation layer), 5. Steuerungsschicht (session layer), 4. Transportschicht (transport layer), 3. Netzwerkschicht (network layer), 2. Datenverbindungsschicht (data link layer), 1. physikalische Schicht (physical layer). Die im Netz zu übermittelnden Daten durchlaufen auf der Senderseite die Schichten von 7 – 1, auf der Empfängerseite in umgekehrter Reihenfolge.
PAP	Password Authentication Protocol. Sicherungsmechanismus innerhalb des PPP zur Authentisierung der Gegenstelle. PAP definiert eine Methode, nach dem Aufbau einer Verbindung anhand eines Benutzernamens und eines Passworts die Rechte des Senders zu prüfen. Dabei geht das Passwort im Klartext über die Leitung. Der Empfänger ver-

	gleicht die Parameter mit seinen Daten und gibt bei Übereinstimmung die Verbindung frei.
PC/SC	Schnittstelle zu Smartcard Readern
PEM	Ältere Form von Soft-Zertifikaten (ohne Private Key).
Personal Firewall	Die Security-Mechanismen der Client Software vereinigen Tunneling-Verfahren und Personal Firewalling. IP-Network Address Translationen (IP-NAT) sowie universelle Filtermechanismen. Von zentraler Bedeutung ist IP-NAT, denn es sorgt dafür, dass nur vom Rechner ins Internet ausgehende Verbindungen möglich sind. Ankommende Datenpakete werden auf der Basis eines ausgeklügelten Filterings nach genau definierten Eigenschaften überprüft und bei Nichtübereinstimmung abgewiesen. Das heißt: Der Internet-Port des jeweiligen Rechners wird vollständig getarnt und der Aufbau von unerwünschten Verbindungen unmöglich.
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard. Verschlüsselungssystem mit öffentlichem Schlüssel.
PKCS#10	Die Form, wie ein Zertifikat vom PKI-Manager an die CA (Certification Authority) übertragen wird. Meist geschieht dies per Http – mit SSL verschlüsselt als Https.
PKCS#11	Basis des Smartcard-Standards
PKCS#12	Soft-Zertifikat. Standard der die Syntax der Dateistruktur beschreibt.
PKCS#15	Pointerbeschreibung: Wo befindet sich was auf der Smartcard.
PKI	(Public Key Infrastructure) Die erforderliche Schlüsselinfrastrukur zur authentischen Verteilung öffentlicher Schlüssel wird PKI genannt. Private und öffentliche Schlüssel werden für asymmetrische Kryptographie verwendet. Transaktionsbezogene Sicherheit erfordert eine eindeutige Partner-Authentisierung mittels Zertifikaten, die von einer vertrauenswürdigen PKI ausgestellt wurden. Insbe-

	sondere für E-Commerce bietet PKI den Rahmen für Vertraulichkeit (Geheimhaltung), Integrität (Fälschungssicherheit), Authentizität (Identitätssicherheit) und Nichtbestreitbarkeit.
PoP	Point of Presence
POP3	Protokoll zum Download von E-Mails. Gegenstück zu SMTP (Port 110)
PPP	Point-to-Point-Protokoll. Übertragunsprotokoll in verbindungsorienten Netzen.
PPP-Verhandlung	Point-to-Point-Protokoll. In einer PPP-Verhandlung wird die IP-Adresse nach Anwahl an den Provider automatisch übergeben.
PRI	Primary Rate Interface (ISDN-Schnittstelle, Primär-Multiplex S2m) mit 30 B-Kanälen und 2 D-Kanälen.
Radius	Remote Authentication Dial In User Service, siehe Directory Service
RA	Registration Authority. Meist ist die Registrierungsstelle die Stelle, die die Daten für die Beantragung eines Zertifikats entgegen nimmt. Die RA ist auch die Stelle, der der Verlust oder der Verfall eines gültigen Zertifikats gemeldet wird und die eine Widerrufsliste (Revocation List) ungültig gewordener Zertifikate herausgibt.
RAS	Remote Access Services. Firmenspezifische (Microsoft) Einwahlhilfe für Remote Access.
RIP	Routing Information Protocol, auch Routing-Modus
RFC	Request for Comment. Normentwurf, Vornorm, die im Internet diskutiert wird und so lange in der Liste der RFCs gehalten wird, so lange sie sich in der Praxis bewährt. Vorformen der RFCs sind Drafts.
Routing-Tabellen	Router benötigen für die Wegewahl im Netz Informationen über die günstigsten Routen von der Quelle zum Ziel. Mit Hilfe der Routing-Tabellen werden diese Strecken vom Router kalkuliert. Während beim statischen Routing die Tabellen fest

vorgegeben sind, erhält der Router beim dynamischen Routing über Router-Informationsprotokolle (z.B. RIP, NLSP, OSPF) Informationen über das Netz, die zu selbst erlernten Routing-Tabellen zusammengesellt werden und ständig aktualisiert werden.

RSA

Das erste Verfahren, das die Anforderungen an die Public Key-Kryptographie erfüllte. Wurde 1977 von Ron Rivest, Adi Shamier und Leonard Adlemann erfunden.

Schnittstelle

(Interface) Festlegung der zwischen zwei Geräten – bei der Datenfernübertragung im allgemeinen zwischen Datenendeinrichtung und Datenübertragungseinrichtung – erforderlichen elektrischen Verbindungsleitungen, der auf diesen herrschenden elektrischen Werten, der zur Funktion erforderlichen Signale sowie der Betriebsweise und Bedeutung dieser Signale. Man unterscheidet nach parallelen und seriellen Interfaces.

SHA

Secure Hash Algorithm, siehe auch Signatur

Signatur

Bei der digitalen Signatur wird mathematisch eine Verknüpfung zwischen Dokument und dem geheimen, persönlichen Signaturschlüssel des Teilnehmers erzeugt. Der Absender des Dokuments generiert eine Prüfsumme (sogenannter Hash-Wert), diese codiert er wiederum mit seinem Geheimschlüssel und erzeugt so einen digitalen Signaturzusatz zur ursprünglichen Nachricht. Der Empfänger des Dokuments kann mit dem öffentlichen Schlüssel des Absenders die Signatur prüfen, indem er seinerseits den Hash-Wert aus der Nachricht bildet und diesen mit der entschlüsselten Signatur vergleicht. Da die Signatur des Absenders unmittelbar in das Dokument eingebunden ist, würde jede spätere Änderung bemerkt. Auch ein Abfangen oder Abhören der Signatur über Lauschangriffe erwiese sich als zwecklos: Die digitale Signatur ist nicht nachahmbar, da sie den geheimen, privaten Schlüssel verwendet; eine Ermittlung des geheimen Schlüssels aus der Signatur ist nicht möglich.

Smartcard Wird die Funktionalität der Smartcard genutzt, so wird nach der CHAP-Authentisierung (User ID und Passwort) die "Erweiterte Authentisierung" (Strong Authentication) mittels der auf Smartcard und Gateway hinterlegten Zertifikate durchgeführt. Auf der Smartcard befinden sich unter anderm das Benutzer-Zertifikat, das Root-Zertifikat und der geheime private Schlüssel. Die Smartcard kann nur mit PIN genutzt werden.

SMTP Simple Mail Transport Protocol. Internet Standard zur Verteilung elektronischer Post. Ist textorientiert und setzt auf TCP auf (Port 25)

SNA Systems Network Architecture. Hierarchisch orientiertes Netz zur Steuerung von Terminals und zur Unterstützung des Zugriffs auf Anwendungen in IBM Host-Systemen.

SNMP Simple Network Management Protocol. Netzwerk-Managementprotokoll auf Basis von UDP/IP.

Source Routing Möglichkeit, in Token Ring-Netzwerken eine Wegewahl zwischen Bridges zu optimieren. Dabei werden die Wegeinformationen an den Datenblock angehängt mit übertragen. Auf diese Weise liegt auch der Weg für die Bestätigung eindeutig fest.

SPD Security Policy Database

SSL Secure Socket Layer. Gemäß dem SSL-Protokoll kann der dynamische Schlüsselaustausch (Dynamic Key Exchange) genutzt werden. SSL, von Netscape entwickelt, ist mittlerweile das Standard-Protokoll für dynamischen Schlüsselaustausch.

SSLCP Secure Socket Layer Control Protocol

STARCOS Betriebssystem für Smartcards

Symmetrische Verschlüsselung Sender und Empfänger verwenden bei der symmetrischen Chiffrierung und Dechiffrierung den gleichen Schlüssel. Symmetrische Algorithmen sind sehr schnell und sehr sicher – dies allerdings nur dann, wenn die Schlüsselübergabe zwischen dem Sender und dem Empfänger ungefährdet erfolgen kann. Gelangt ein Unbefugter in den Besitz des Schlüssels, so kann dieser alle Nachrichten ent-

schlüsseln bzw. sich unter Verwendung des Schlüssels als Absender von Nachrichten ausgeben. Soll bei der symmetrischen Verschlüsselung in größeren Gruppen jeder Teilnehmer nur an ihn adressierte Nachrichten lesen können, so ist für jedes Sender-Empfänger-Paar ein eigener Schlüssel notwendig. Die Folge: ein aufwendiges Schlüsselmanagement. So sind bei 1.000 Teilnehmern bereits 499.500 (!) unterschiedliche Schlüssel erforderlich, um sämtliche Wechselbeziehungen zu unterstützen. Bekannteste symmetrische Verschlüsselung ist heute der DES-Algorithmus.

TCP/IP

Transmission Control Protocol / Internet Protocol. TCP/IP ist ein Netzwerkprotokoll für heterogene Netze und an kein Transportmedium gebunden. Es kann auf X.25, Token Ring oder einfach auf die serielle Schnittstelle aufsetzen und eignet sich deshalb besonders als Kommunikati-onsprotokoll für unterschiedliche (Netz-) Topologien und Rechner-Plattformen, wie sie im Internet gekoppelt sind. Dabei wird jeder Rechner im Netzverbund Internet durch seine IP-Adresse identifiziert. TCP/IP umfaßt außerdem vier Internet-Standardfunktonen: 1. FTP: File Transfer Protocol für den Dateitransfer von einem zum anderen Rechner, 2. SMTP: Simple Mail Transport Protocol für E-Mail, 3. TELNET: Teletype Network für Terminalemulation, 4. RLOGIN: Remote Login zur Rechnerfernbedienung

TECOS

Betriebssystem für Smartcards (Versionen 1.2, 2.0)

Token Ring

Netzwerktopologie mit Ringstruktur von IBM.

UDP

User Data Protocol. Baut direkt auf dem darunter liegenden Internet Protokoll auf. Wurde definidert, um auch Anwendungsprozessen die direkte Möglichkeit zu geben, Datagramme zu versenden. UDP liefert über die Leistungen von IP hinaus lediglich eine Portnummer und eine Prüfsumme der Daten. Durch das Fehlen des Overheads mit Quittungen und Sicherungen ist es besonders schnell und effizient.

UMTS	Universal Mobile Telecommunications Service. Künftiger Standard für schnelle Handy-Kommunikation.
VPN	Virtual Private Network. Ein VPN kann als virtuelles Netz grundsätzlich über alle IP-Trägernetze – also auch das Internet – eingerichtet werden. Für die Realisation haben sich zwei Spezifikationen herauskristallisiert: L2F (Layer 2 Forwarding) und L2TP (Layer 2 Tunneling Protocol). Beide Verfahren dienen dazu, einen Tunnel aufzubauen, den man als eine Art “virtuelle Standleitung” bezeichnen kann. Über eine solche logische Verbindung lassen sich neben IP-Frames auch IPX-, SNA- und NetBIOS-Daten transparent übertragen. Am Tunnelende müssen die Datenpakete interpretiert und zu einem Datenstrom auf der Basis des verwendeten Protokolls umgewandelt werden.
WAP	Wireless Application Protocol. Entwicklung von Nokia, Ericson und Motorola.
X.509 v3	Standard Zertifizierung
Zertifikate	Zertificate (Certificates) werden von einer CA (Certification Authority) mit-tels PKI-Manager (Software) ausgestellt und auf eine Smartcard (Chipkarte) gebrannt. Diese Smartcard enthält u.a. mit den Zertifikaten digitale Signaturen, die ihr den Status eines digitalen Personalausweises verleihen.

Index

E

F

G

H

I

R

S

T

U

V

W

X

Z